United Arab Emirates University
Scholarworks@UAEU

Theses | Electronic Theses and Dissertations

11-2020

ESTABLISHING BLOCKCHAIN-RELATED SECURITY CONTROLS

Maitha Ali Mohammed Hamad Al Ketbi

Follow this and additional works at: https://scholarworks.uaeu.ac.ae/all_theses

 Part of the Information Security Commons

Recommended Citation

Al Ketbi, Maitha Ali Mohammed Hamad, "ESTABLISHING BLOCKCHAIN-RELATED SECURITY CONTROLS" (2020). *Theses*. 814.
https://scholarworks.uaeu.ac.ae/all_theses/814

This Thesis is brought to you for free and open access by the Electronic Theses and Dissertations at Scholarworks@UAEU. It has been accepted for inclusion in Theses by an authorized administrator of Scholarworks@UAEU. For more information, please contact mariam_aljaberi@uaeu.ac.ae.

United Arab Emirates University

College of Information Technology

Department of Information Systems and Security

ESTABLISHING BLOCKCHAIN-RELATED SECURITY CONTROLS

Maitha Ali Mohammed Hamad Al Ketbi

This thesis is submitted in partial fulfilment of the requirements for the degree of Master of Science in Information Security

Under the Supervision of Professor Khaled Shuaib

November 2020

Declaration of Original Work

I, Maitha Ali Mohammed Hamad Al Ketbi, the undersigned, a graduate student at the United Arab Emirates University (UAEU), and the author of this thesis entitled "*Establishing Blockchain-Related Security Controls*", hereby, solemnly declare that this thesis is my own original research work that has been done and prepared by me under the supervision of Professor Khaled Shuaib, in the College of Information Technology at UAEU. This work has not previously been presented or published, or formed the basis for the award of any academic degree, diploma or a similar title at this or any other university. Any materials borrowed from other sources (whether published or unpublished) and relied upon or included in my thesis have been properly cited and acknowledged in accordance with appropriate academic conventions. I further declare that there is no potential conflict of interest with respect to the research, data collection, authorship, presentation and/or publication of this thesis.

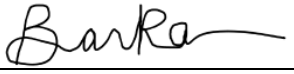
Student's Signature:  Date: __15/11/2020_____

Copyright © 2020 Maitha Ali Mohammed Hamad Al Ketbi
All Rights Reserved

Approval of the Master Thesis

This Master Thesis is approved by the following Examining Committee Members:

1) Advisor (Committee Chair): Khaled Shuaib
   Title: Professor
   Department of Information Systems and Security
   College of Information Technology
   Signature  Date 15/11/2020

2) Member: Ezedin Barka
   Title: Associate Professor & Chair
   Department of Information Systems and Security
   College of Information Technology
   Signature  Date 15/11/2020

3) Member: Marton Gergely
   Title: Assistant Professor
   Department of Information Systems and Security
   College of Information Technology
   Signature  Date 16/11/2020

4) Member (External Examiner): Moayad Aloqaily
   Title: Assistant Professor & Program Director
   Department of Cybersecurity
   Institution: Al Ain University, UAE
   Signature  Date 16/11/2020

This Master Thesis is accepted by:

Dean of the College of Information Technology: Professor Taieb Znati

Signature Taieb Znati Date January 7, 2021

Dean of the College of Graduate Studies: Professor Ali Al-Marzouqi

Signature Ali Hassan Date January 7, 2021

Copy ____ of ____

Abstract

Blockchain technology is a secure and relatively new technology of distributed digital ledgers which is based on interlinked blocks of transactions. There is a rapid growth in the adoption of the blockchain technology in different solutions and applications and within different industries throughout the world, such as but not limited to, finance, supply chain, digital identity, energy, healthcare, real estate and government. Blockchain technology has great benefits such as decentralization, transparency, immutability and automation. Like any other emerging technology, the blockchain technology has also several risks and threats associated with its expected benefits which in turns could have a negative impact on individuals, entities and/or countries. This is mainly due to the absence of a solid governance foundation for managing and mitigating such risks and the shortage of published standards to govern the blockchain technology along with its associated applications. In line with the "Dubai blockchain Strategy 2020" and "Emirates blockchain Strategy 2021" initiatives, this thesis aims to achieve the following: first, preservation of the confidentiality, integrity and availability of information and information assets in relevance to blockchain applications and solutions implementation across entities, and second, mitigation and reduction of related information security risks and threats; through the establishment of new information security controls specifically related to the blockchain technology which have not been covered in International and National Information Security Standards which are ISO 27001:2013 Standard and UAE Information Assurance Standards by the Signals Intelligence Agency (formerly known as the National Electronic Security Authority). Finally, Risk Assessment and Risk Treatment have been performed on five blockchain use cases; to determine their involved risks with respective to security controls appropriately. The assessment/analysis results showed that the proposed security controls can mitigate relevant information security risks on the blockchain solutions and applications and consequently protect the information and information assets from unauthorized disclosure, modification, and destruction.

Keywords: Blockchain technology, Standards, Security controls, Information security, Security governance.

Title and Abstract (in Arabic)

إنشاء ضوابط أمنية متعلقة بتقنية البلوك تشين

الملخص

تعد تقنية البلوك تشين (blockchain) تقنية آمنة وجديدة نسبياً متمثلة فيما يسمى بالدفتر الرقمي الموزع (distributed digital ledgers) من الكتل المترابطة من المعاملات الرقمية. إن هذه التقنية قد نمت وبشكل سريع حول العالم حيث تم اعتمادها في العديد من الحلول والتطبيقات الفنية ضمن مختلف الصناعات، على سبيل المثال لا الحصر، في قطاع المالية والتوريد والهوية الرقمية والطاقة والرعاية الصحية والعقارات والخدمات الحكومية. تتمتع تقنية البلوك تشين بفوائد عظيمة مثل اللامركزية والشفافية والأتمتة والثبات/عدم قابلية التغير. ولكن مثل أي تقنية أخرى ناشئة، فإن تقنية البلوك تشين لديها أيضاً العديد من المخاطر والتهديدات المرتبطة بفوائدها العظيمة والتي بدورها قد يكون لديها تأثير سلبي على الأفراد و/أو الجهات "قطاعات الأعمال" و/أو على الدول بشكل عام. هذا يرجع أساساً إلى عدم وجود أساس قوي ومتين لحوكمة وإدارة هذه المخاطر والحد منها بالإضافة إلى قلة المعايير المنشورة لإدارة هذه التقنية وتطبيقاتها ذات الصلة. وتماشياً أيضاً مع استراتيجيات حكومة دولة الامارات لتقنية البلوك تشين وهي: استراتيجية دبي للتعاملات الرقمية ٢٠٢٠ واستراتيجية الإمارات للتعاملات الرقمية ٢٠٢١، فقد تهدف هذه االرسالة إلى تحقيق ما يلي: أولاً، الحفاظ على أمن المعلومات وأصول المعلومات المتعلقة بتنفيذ تطبيقات وحلول تقنية البلوك تشين في الجهات وذلك من خلال ضمان سريتها وسلامتها وتوفرها. وثانياً، معالجة مخاطر أمن المعلومات ذات الصلة والحد منها. وسيتم تحقيق هذين الهدفين من خلال إنشاء ضوابط أمن معلومات جديدة خاصة بتقنية البلوك تشين لم يتم تغطيتها في المعايير الدولية والوطنية لأمن المعلومات: المعيار الدولي لأمن المعلومات (آيزو ٢٧٠٠١ – ISO 27001) والمعيار الوطني لضمان المعلومات الصادر من جهاز استخبارات الإشارة (المعروف سابقاً بالهيئة الوطنية للأمن الإلكتروني). أخيراً، تم إجراء تقييم ومعالجة المخاطر في خمس من حالات استخدام تقنية البلوك تشين (blockchain use cases)؛ من أجل تحديد المخاطر المرتبطة بها مع الضوابط الأمنية المناسبة ذات الصلة. وبالتالي، أظهرت نتائج التحليل/التقييم أن الضوابط الأمنية المقترحة تساهم في الحد من المخاطر المرتبطة بتطبيقات وحلول تقنية البلوك تشين وحماية المعلومات وأصول المعلومات من الكشف والتعديل والاتلاف غير المصرح به.

مفاهيم البحث الرئيسية: تقنية البلوك تشين (blockchain)، المعايير، الضوابط الأمنية، أمن المعلومات، الحوكمة الأمنية.

Acknowledgements

First of all, I would like to express my sincere thanks and appreciation to my thesis advisor Professor Khaled Shuaib for his great guidance, support, and assistance throughout my preparation of this thesis. In addition, many thanks for the Examining Committee Members for their acceptance to be part of this committee, their willingness to serve on it and their contribution for enhancing my thesis.

I would like to thank all people who tried their best while I searched for a specific detail regarding the blockchain use cases and/or solutions which are implemented in UAE. And also, I would like to thank all the professional advisors and consultants for their help, support and useful discussion that I had with them regarding my thesis, to my direct manager Dr. Khaled Alawadhi and all my colleagues at work for their support and encouragement.

Last but not least, a very special thanks to my parents and all my family members (especially my grandmothers, sisters, brothers and husband) who continuously support and encourage me; your presence is the best blessing in my life.

Dedication

To my beloved parents, family and country.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AMHL	Anonymous Multi-Hop Locks
BaaS	Blockchain-as-a-Service
BC	Blockchain
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CICMP	Common Inter-Chain Messaging Protocol
DAO	Decentralized Autonomous Organization
DLT	Distributed Ledger Technologies
IEEE	Institute of Electrical and Electronics Engineering
IEEE SA	IEEE Standards Association
IETF	Internet Engineering Task Force
ISITC	International Securities Association for Institutional Trade Communication
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
RAND	Europe Research and Development

SDO	Standards Developing Organization
UAE IA Standards	UAE Information Assurance Standards
W3C	World Wide Web Consortium

Chapter 1: Introduction

1.1 Overview

The blockchain technology is considered as one of the Distributed Ledger Technologies (DLT), that its applications have been grown rapidly in finance, supply chain, digital identity, energy, healthcare, real estate and government. This rapid adoption is due to its expected great benefits in term of achieving decentralization, transparency, immutability and automation environment. The Deloitte report on "Global Blockchain Survey, 2019" shows that 53% of the global enterprises consider the blockchain technology to be critical and it is on the top of their strategic priorities. In addition, it shows that more than 40% approximately of global enterprises are planning to invest and spend $5 million dollars on blockchain solutions during the next 12 months [1]. In the research field; there is a good number of published research papers proposing the adoption blockchain technology in different industries. Examples of recent and most published papers regarding this of the current year 2020 are the following: [2-4] in supply chain, [5-7] in healthcare, [8-10] in energy.

1.2 Statement of the Problem

Blockchain technology involves many risks and threats that require a serious attention from a governance and management perspectives which unfortunately do not exist. Thus, one of the main problems related to the adoption of blockchains and distributed ledger technologies is the absence of needed solid foundation in governance for such technologies [11, 12]. Currently, there is an acute shortage of published standards related to governing these technologies and their associated applications in order to better achieve the intended benefits and thus maintain a long-term survival and adoption strategy of these technologies. The Gartner Inc. report

regarding “Hype Cycle for Blockchain Technologies, 2020” including Figure 1 shows that blockchain technology is falling into the “Trough of Disillusionment” and most of blockchain technologies need for 2 to 5 years to become fully scalable technically and operationally [13, 14].

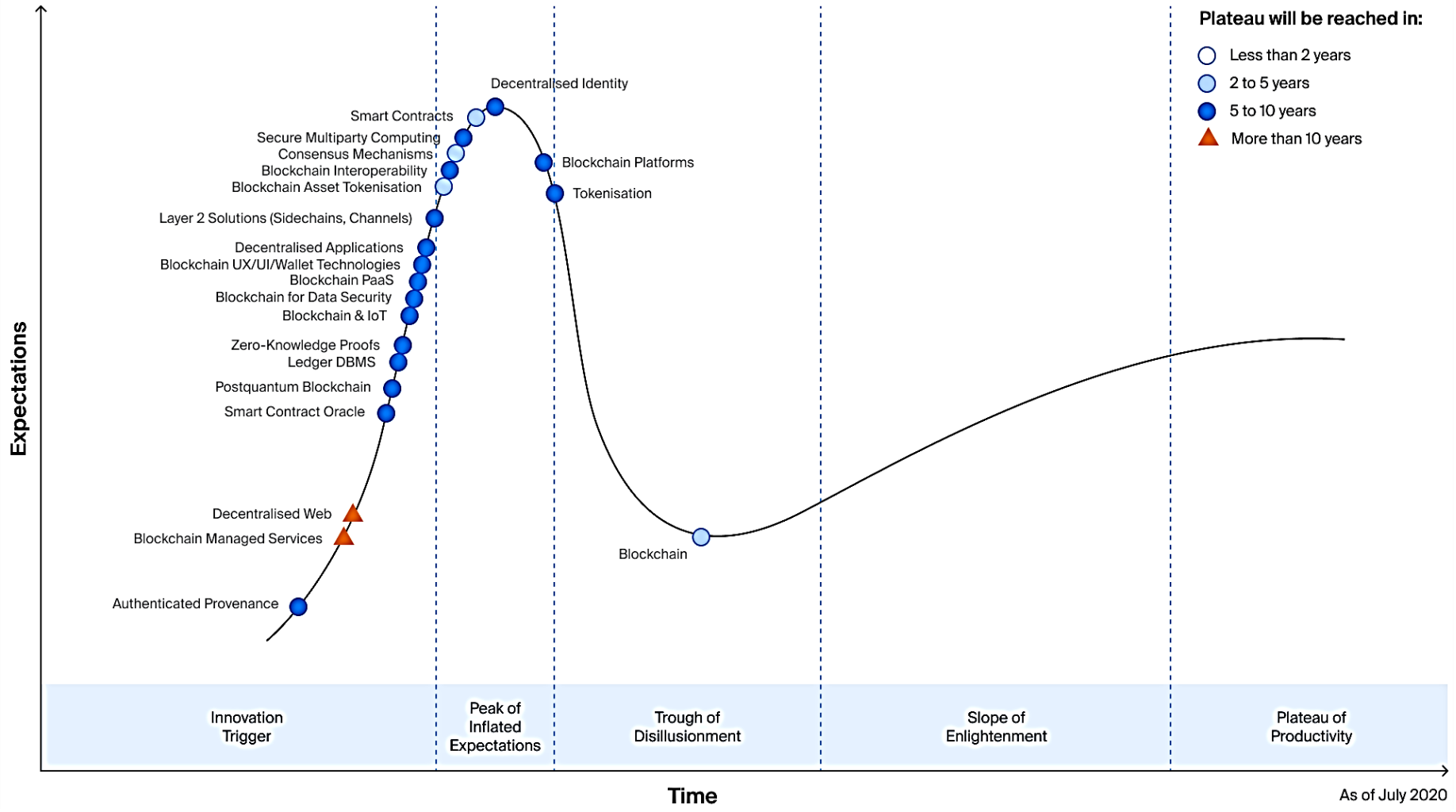


Figure 1: Hype Cycle for Blockchain Technologies, 2020 (Source: [14])

In order to maintain and ensure the scalability, interoperability, flexibility, and governance of the blockchain technology, a set of relevant standards should be developed. Based on that, there are many standards developing organization (SDO) throughout the world responsible for developing standards in general such as, but not limited to the following: International Organization for Standardization (ISO), ITU Telecommunication Standardization Sector (ITU-T), IEEE Standards Association, World Wide Web Consortium (W3C). SDOs realize the lack of standardization in relevant to the blockchains technology and its implications on the short and long terms. Thus, they understand the importance and the need of creating relevant standards that require the contribution of SDOs and the involvement of subject matter experts globally and thus consensus on developing common sets of relevant standards properly while ensuring to cover different aspects of the technology. The proposed standards cover various aspects such as but not limited to: definitions, implementation, management, cyber security and core attributes (including data). However, one major drawback in the development of standards is that it requires a long time to release a standard. As of today, most of planned relevant standards are currently under development. (For further information about two main SDOs “which are ISO and IEEE Standards Association” that are directly and/or indirectly responsible for the development of the relevant standards “as a list”, see Appendix).

Therefore, this thesis aims to address the problem of the lack of governing information security risks related to blockchain technology implementation by establishing new information security controls specifically related to the blockchain technology that have not been covered by International and National Information Security Standards which are ISO 27001:2013 Standard and UAE Information Assurance Standards by Signals Intelligence Agency (formerly known as the National

Electronic Security Authority). Consequently, this is will ensure the information and information assets are protected against possible unauthorized disclosure, modification, and destruction which could have a negative impact on individuals, entities and/or national levels.

1.3 Thesis Motivation

The United Arab Emirates is considered as one of the leading countries in the world that always seeks into adapting the latest solutions and applications in advanced technology; in order to support and achieve the UAE trends and directions into providing and sustaining its services across different sectors. With respect to the blockchain technology, the UAE government launched two initiatives. The first is the "Dubai Blockchain Strategy 2020" which was launched in October 2016 by H.H. Sheikh Mohammed bin Rashid Al Maktoum, aiming to make Dubai "the first city fully powered by blockchain by 2020 and the happiest city on earth" via achieving the following three strategic pillars: government efficiency, industry creation and international leadership [15]. The second is the "Emirates Blockchain Strategy 2021" which was announced in April 2018 and aims for 50% digital transformation of the UAE government's transactions using the blockchain platform by 2021 [16]. Therefore, the motivation behind this thesis is to participate and contribute in achieving the vision and mission of the "Dubai Blockchain Strategy 2020" and "Emirates Blockchain Strategy 2021" via mitigating the associated information security risks of the UAE-based blockchain projects implemented in line with the relevant two initiatives.

Finally, the structure of this thesis as per the following: Chapter 2 presents an overview of the blockchain technology, Chapter 3 presents a summary and discussion

of the literature review, Chapter 4 presents the establishment of security controls, Chapter 5 presents the analysis and discussion including a proposed evaluation process and lastly Chapter 6 concludes the thesis and presents the future work.

Chapter 2: Overview of Blockchain Technology

Blockchain technology is a peer to peer network of the digital ledger distributed across the entire network of computer systems without a central authority (or a third party) to manage the respective network. It is one type of Distributed Ledger Technology (DLT) that its applications have been grown rapidly in finance, supply chain, digital identity, energy, healthcare, real estate and government. The main properties of the blockchain technology are the following:

1. Decentralized: Which eliminate the centralization issue which is the single point of failure. Thus, all nodes on the network have a copy of the ledger so it will never be fully shut down in case of the denial of service.
2. Immutable: Once the block has been added on the blockchain, it can't be tampered with. Since, the block is cryptographically linked to the previous one.
3. Transparence: The identity of the participant is either anonymous or pseudonymous. It is represented as a public address instead of using the real identity, thus it is hidden.

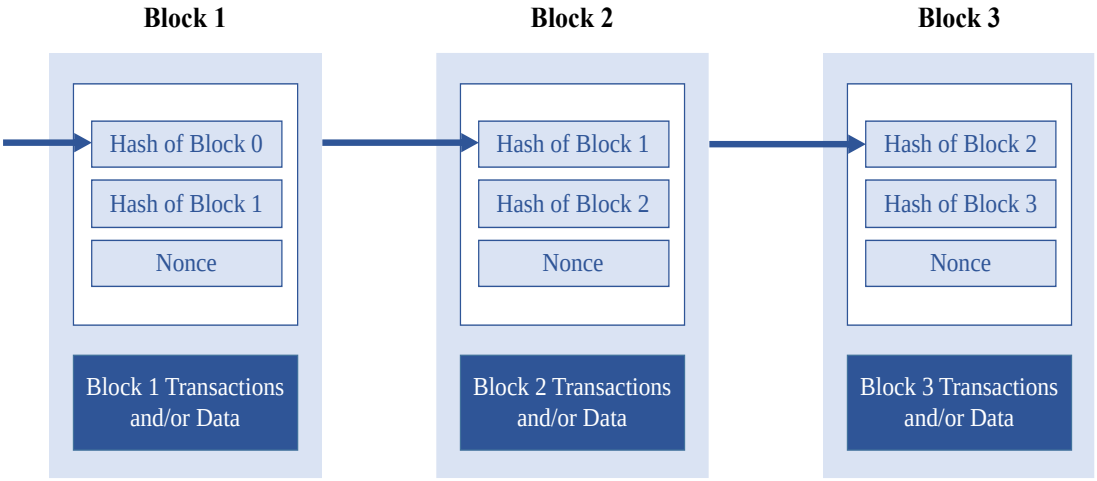


Figure 2: Block Components

Blockchain is a chain of blocks which contains a set of different transactions. Each block is cryptographically linked to the previous one. In addition, each block contains data (for example, set of transactions), the hash of the block, the hash of the previous block and the nonce (which is a random number, if applicable) as shown on Figure 2.

2.1 Consensus Models

Before the block is added to the chain of the previous blocks on the network, it goes through a validation process. The majority of the participant should agree on the validity of the block which is called group consensus and/or consensus models. There are many types of the consensus models such as but not limited to the following:

- Proof of Work (PoW) Consensus Model

  It is designed for a system that there is little or no trust among its users as the public/permissionless blockchain. Nodes are competing to solve the mathematical problem (a puzzle) which require resource consumption known as miners; thus, the winner will get incentive and rewarded accordingly. Difficulty is adjusted by the network to correspond to load, this is will ensure no one on the network can take over the block production thus prevent 51% attack. They have to guess the correct nonce that the computational result “hash output” of the block data and guessed nonce matches the difficulty level.

- Proof of Stake (PoS) Consensus Model

  It is a new proposed and alternative model to Proof of Work (PoW) due to its limitations such as higher energy consumption and slower transaction speed. It uses a stake for reward the validators. The nodes who wish to participate on the block's validation should give or pay a stake. A random node is selected; thus, it

should show the hash output of the block to all other participant. If all of them agree on the validity of the output, then the selected node (random node) will get rewarded according to all who wagered on that node, if not then it will not get rewarded and will loses his stake and therefore a new random node will be selected.

- Proof of Authority (PoA) Consensus Model

  This is an alternative consensus model of Proof of Work (PoW) however it is only for private blockchain. It uses a set of authorities/validators in order to validate the blocks and maintain the blockchain's security.

- Proof of Burn Consensus Model

  The coins are burned through sending these burned coins to an address where they can't be retrieved. The more coins burned, the more likely to be selected for mining the next block.

- Proof of Activity Consensus Model

  It is a combination of the Proof of Work (PoW) and Proof of Stake (PoS) consensus models. Blocks are mined using Proof of Work (PoW) and the transactions are validated using Proof of Stake (PoS).

- Proof of Capacity Consensus Model

  If the validators want to participate into mining the next block, the hard drive space is required to be staked. The most space staked by the validator, the more likely to be selected to mine the next block.

- Proof of Elapsed Time Consensus Model

  It is similar to Proof of Work (PoW) consensus model however it consumes less energy thus it is more energy efficient. It is created and govern by Intel.

2.2 Blockchain Types

Blockchain technology has three main types which are public, private and consortium blockchain. The following is the detailed description for each type.

1. Public Blockchain

   Everyone on the network can access and add a record. In addition, anyone can create and validate the block and/or transaction. Thus, the network is fully decentralized and permissionless. The participant is anonymous therefore their identity is hidden. The consensus algorithm is depending on a group consensus, such as but not limited to, Proof of Work (PoW) or Proof of Stake (PoS).

2. Private Blockchain

   It is permissioned network owned and governed by an individual or organization. Therefore, the respective organization is responsible for providing the relevant permission for access, validate, view transactions to authorized participants. Thus, it is not fully decentralized network. The identity of participant is known. The consensus model is depending on the respective organization's directions, or through a voting or multi-party consensus algorithm. It is easier to validate the transactions thus it is faster.

3. Consortium Blockchain

   It is governed and owned by multiple organizations. Thus, the permission is granted by a group of respective organizations to pre-selected nodes to read and write on the respective network. The consensus model is achieved through a voting or multi-party consensus algorithm in order to create, validate, and review the block and/or transaction. It is similar to private blockchain type in term of the efficiency and privacy [17, 18].

2.3 Security Risks

The most blockchain security risks are private key, malware vulnerability, network, and smart contract. The following are the detailed information about each one of them.

- Private Key Security

  Blockchain technology use public key cryptography which involve having the respective user two binding keys one is public and the another is private key. The private key is used for signing the transactions. Therefore, the failure to protect user private key from loss can leads to unable to reach the respective account that holds the relevant assets, and failure to protect it from stolen, and/or hacking as well by another party can leads to impersonate the respective user thus generate a valid signature on behalf of him and losing the digital assets of that account as well (for example, cryptocurrency coins).

- Malware Vulnerability

  Users use their computer/machine to access blockchain network and use the services that are available on the respective platform. The infected user's machine by malware can effect on the blockchain security through attacking the nodes that are on the respective network, using the computer resources to perform Proof of Work (PoW) mining process therefore taking control of the respective network and taking control of user's control since the private key is stored on his computer.

- Network Security

  The blockchain security is depend on the security of the underlying infrastructure such as flawed network design and poor network security. Therefore, the underlying infrastructure of the respective blockchain network should be design

properly in order to meet the blockchain requirements such as but not limited to bandwidth, physical and logical security and etc.

- Smart Contract Security

  The smart contract is a code of program that executed once the predefined conditions are met. It is stored and executed on the blockchain network. Like any other program, smart contracts are vulnerable to threats, vulnerabilities, security holes and bugs. Therefore, the smart contract code is not trusted and could be malicious [19, 20].

Chapter 3: Literature Review

There is lack of research papers in the area of security governance of the blockchain technology in terms of developing blockchain standards and/or establishing relevant security controls. The study by Nusi et al. [12] states that "The number of sources specifically focused on risk management for adoption, requirements engineering and standards-based use of blockchain technology remains comparably low" Moreover, the study states also that "Regarding the current research in the area of risk management within the adoption and standards-based application of blockchain technology. It showed that the research landscape around this topic is still in its early stage, resulting in large research gaps throughout the field" [12]. Thus, the seven sighted studies in this chapter are either generally or specifically focus on the proposed work. In addition, this chapter summarizes these studies and discusses their limitations in this regard and with respect to this field and compares them with the work that has been done as part of this thesis.

The study by Gaby et al. [21] proposed a framework called "Ancile" which is an Ethereum-based blockchain framework with its main purpose focused on meeting legislative standards specifically related to protecting patient's privacy. For example, the compliance with the Health Insurance Portability and Accountability Act (HIPPA) requirements via managing and controlling the access to the Electronic Health Record (EHR) of patients through the use of encryption and authentication mechanisms of blockchain technologies thus preserving the privacy of their sensitive information. However, not all information is concealed completely hence the level of concealment depends on the implementation. This is usually achieved through the use of smart contracts, also via tracking the usage of the medical records, secure transfer of medical

records and the prevention of unauthorized access of Protected Health Information (PHI). Therefore, the preservation of patients' privacy and security in compliance with regulations and interoperability guidelines need to be strongly considered. Ancile as a permissioned blockchain will delegate some nodes with a higher authority. Ancile can replace the existing systems effectively in terms of both cost and storage. However, due to the patient's ownership right over his data, data can't be used as an incentive, in other words, as an exchanged currency for miners [21].

The study by Lima [22] highlights the methodology to develop a framework related to DLT standards through three steps in an iterative process. The first step of this top-down approach is to define an initial reference model in order to create a system-of-systems model thus identifying the key subsystem components of the technology which are the stakeholders, concerns, architectural viewpoints, and systems of interest. The second step is to identify industrial use cases in order to map it with the created model. Lastly, the created model is revised, refined, iterated and improved. Another approach is to start with the second step which is to identify industrial use cases thus going with the same previous sequence, however this approach has a drawback of the lack of 360° view which can be achieved with the first approach.

Moreover, this study classifies the DLT/blockchain standards into four categories based on the following criteria: the viewpoints, level of depth, boundaries, demarcation points, and the industrial collaboration for each part in the system (including the subsystems) of the technology.

The first category called "Generic Framework Standards" which is considered as a starting point of developing standards for all new technologies and as a foundation

of the subsequent standards categories. It focuses on Reference Guide, Reference Frameworks, Architectures, Terminologies, Interfaces, Ontology, Classification, etc. This type of standard can involve an iterative approach of refining and validating the preliminary assumptions of an initial model through use cases. Working groups and committee examples of this type of standards are IEEE DLT/blockchain standards, ISO/TC 307 on blockchain and distributed ledger technologies, and ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT).

The second category called “Enabling Technology Standards” which is mainly focusing on technology related mechanisms including but not limited to the followings: Client Interfaces, Identity Management, Data Formats, Consensus Algorithm, Token Specifications … etc. Examples of this type of standards are created by institutions such as: The Institute of Electrical and Electronics Engineers (IEEE), The World Wide Web Consortium (W3C), The Enterprise Ethereum Alliance (EEA) and The International Telecommunication Union (ITU).

The third category called “Platform-Specific Standards”, is relevant to the previous type of Enabling Technology Standards, however it is platform-based focuses on a higher level of systemic view. Well-known implementation examples include Ethereum, Hyperledger, Corda, etc. It also covers another category of cloud-based solutions known as Blockchain-as-a-Service (BaaS). Popular examples include but not limited to IBM, Microsoft, Amazon, VMWare.

The last category called “Vertical-Industry-Specific Standards” which is mainly an establishment of specific industrial use cases standards based on the first type of Generic Framework Standards. It focuses on blockchain’s applications such as energy, health care, telecom/IT, manufacturing, supply chain, logistics and

transportation. Key success of its creation highly depends on the required involvement, knowledge, and expertise of each industry.

Furthermore, this study proposes a high level of Blockchain Architecture Framework using ISO/IEC/IEEE 42010 “Systems and software engineering – Architecture description” as a reference model through applying the three steps mentioned previously which are: creating a system-of-systems model in line with this selected reference model and identifying the key components of stakeholders, concerns, architectural viewpoints, and systems of interest, then mapping the created model with the selected industrial use cases, and lastly, revising, refining, iterating and improving the model. Its implementation type is considered as part of the Generic Framework Standards [22].

The study by John and Adrian [23] discusses three key areas of concern that should be covered while developing the standards, namely, blockchain governance, smart contracts and interoperability between and across blockchains.

The first area, “blockchain governance”, includes the following aspects: standards, data, key security and smart contracts. Its failure can impact negatively on the advancement of distributed ledger technology. Real failing examples of the used consensus algorithm are the forking of Bitcoin and Bitcoin Cash as well as Ether and Ether classic. In term of data governance, it is crucial to ensure that the confidentiality and privacy of the data are not compromised within the desired blockchain architecture. In addition, complying with relevant standards such as the European Union’s General Data Protection Rules (GDPR), through ensuring that no Personal Identifiable Information (PII) is stored on the blockchain itself is a must. However, PII can only be stored off-chain in a separate data repository which can be accessible

through blockchain environment. Thus, this also falls under sensitive information that an organization has/owns. In the case of using permissioned blockchain (consortium) type, a common standard for data management and governance should be agreed upon by the members. For example, when a member exiting from the network, an exit agreement should be available for terminating his activities, services, etc. Another aspect which has been mentioned in this area is key security which focus on the protection of the used private key from being hacked through using certificated and cracked proof hardware wallets or offline hardware security modules as per the relevant standards compliance such as US Government FIPS 140-2 level 3 certification.

The second area, “Smart contracts”, where a written code is considered as a governing law by the blockchain communities while might be different from a legal perspective. Moreover, smart contracts are error prone, for example, Decentralized Autonomous Organization (DAO) code that had major vulnerabilities of implementing a hard fork on the Ethereum blockchain in May 2016. Another issue in smart contracts is interoperability for communication within the blockchain and with other blockchains.

The third and last area, “Interoperability across blockchains”, is defined in terms of cross-chain interoperability and enterprise system integration and interoperability as well, taking into considerations data access and storage (including off-chain). This includes the following aspects: interoperability of the smart contract, cross-chain and sidechains. Interoperability in terms of smart contracts can impact their performance and outcomes based on internal and external factors but mainly due to the lack of interoperability across different blockchains. The second aspect is

establishing secure and trusted interactions between cross-chains (including value transfer) by using different solutions such as Common Inter-Chain Messaging Protocol (CICMP) and Anonymous Multi-Hop Locks (AMHL). The last aspect is the interoperability of sidechains which enable digital tokens movements across different blockchains securely [23].

The study by Kiran et al. [24] states that organizations should identify and understand risks involved when deploying a blockchain/DLT technology. It highlights six risks on a high-level overview which might affect negatively the implementation and adoption of the blockchain technology within the existing organization operations and systems. The risks are scalability, technology implementation and acquisition, data security and confidentiality, regulatory hurdles, jurisdiction and storage limitation.

Therefore, in order to mitigate the associated risks of this technology and ensure data security, confidentiality, privacy, and accountability within the organizations; an effective risk management strategy should be established, implemented and monitored properly, as well as through enhancing the information technology controls taking into considerations the following five areas: information security policies, physical security, key management and cryptography controls, computer operations and lastly, logical access controls. In addition, this study highlights six key blockchain areas which are: platform, nodes, development, user, security incidents and asset management, along with its involved risks and respective controls in a high-level overview that organizations have to focus on in order to achieve a secure environment of blockchain.

This study highlights also the key areas to be considered by the organizations while integrating applications related to the desired blockchain technology. Firstly,

“Data conversion and legacy system integration”, which states that organizations should perform the required analysis of already existing platforms they have/own such as web servers, databases, mainframes, outsourced applications and Identity and Access Management (IAM) solutions, before integrating blockchain/DLT solutions and application with its IT systems. In order to maintain transforming and loading data properly, accurately and completely into the new integrated systems thus ensuring readability through the used interfaces (including, blockchain/DLT interfaces). Secondly, “Key management for logical access” which states that organizations should implement the Public Key Infrastructure (PKI) solutions effectively in order to protect and maintain the security of the user’s access keys (public and private keys) to the ledger file or interfaces. In addition, the organizations that use a public permissioned blockchains type, also known as a hybrid permissioned blockchains, need to take into considerations managing the consensus algorithm operation effectively and protecting its integrity. Lastly, “Access considerations for hardware security”, which is related to the pervious area however it focuses on the physical security of hardware-based tokens that store the private’s keys, such as physical badges, PIV/CIV cards, and biometric authentication mechanisms. Thus, it requires a comprehensive approach regarding its security and management [24].

The study by Vincent and Mark [25] proposed a high-level description regarding the three elements that should be covered on the blockchain-based functional architecture. The relevant elements are consensus, security and ownership elements. The description of the consensus element focused on the importance of the global agreement on the block publication process and its content. Also, the description of the security element highlighted the important of preventing malicious users from tampering and taking over asset's ownership of a user. Last, the description of the

ownership element focused on the tracking the asset's ownership through the respective addresses or accounts. The highlighted different transaction models across various blockchain applications, also they highlighted the smart contract in term of the legal aspects, token and programming languages.

Also, they highlighted the list of the international and regional Standards Developing Organizations (SDOs) and their efforts into developing blockchain related standards in order to maintain interoperability, scalability and compatibility but the majority are currently still under progress/development. The relevant organizations are the International Organization for Standardization (ISO), International Telecommunication Union (ITU), World Wide Web Consortium (W3C), Institute of Electrical and Electronics Engineering (IEEE), Internet Engineering Task Force (IETF), Standards Australia, International Securities Association for Institutional Trade Communication (ISITC) Europe, Research and Development (RAND), European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC), and National Institute of Standards and Technology (NIST).

In addition, they highlighted the lack of common terminology with the respect of the blockchain technology which is currently under considerations and establishment by the respective technical committee of the International Organization for Standardization (ISO). Therefore, they mentioned the following terms: Blockchain, Clients and Servers, Consensus, Pseudonymity, and they proposed a terminology for each one [25].

With the respect of the standards, the study by Rafael and Rocco [26] reviewed the existed standards in relation to the decentralized cloud solutions that could benefit

from them in order to maintain and improve the compatibility between various relevant projects. Thus, they briefly described decentralized clouds requirements for which are the following: service definition, smart contracts for Quality of service (QoS), execution flow, management of components, data elements, data privacy, federated clouds, distributed ledger. Lastly, they briefly highlighted the ongoing initiatives by international Standards Developing Organizations (SDOs) [26].

Lastly, the study by James and Maria [27] evaluated four major blockchain platforms in term of their compliance with National Institute of Standards and Technology (NIST) cryptographic standards as per Federal Informa-tion Security Management Act of 2002 (FISMA) requirements. Taking into considerations the following criteria which are applicable for almost any blockchain project. First, it should be managed and supported by single entity. Also, it should allow for independent private chains instead of having a single global network. Last, it should be supported by the libraries that allow for an easy access to data and protocols related to blockchain technology. The relevant standard includes the following which are in relation to blockchain implementation: cryptographic hashing, digital signatures, and pseudorandom number generators (PRNGs). Each have been mentioned in detail along with their relevant algo-rithms. In addition, the relevant platforms which have been evaluated are Ethereum, Hyperledger Fabric, R3's Corda and Multichain. Finally, the evaluation results showed that R3's Corda meets the relevant NIST requirements [27].

All the aforementioned reviews show that both of the first two studies proposed a blockchain-based framework. The first study by Gaby et al. [21] proposed a blockchain-based framework in line with regulatory standards related to patient's privacy protection such a regulation called HIPPA. The second study by Lima [22]

also proposed a high level of Blockchain Architecture Framework in line with ISO/IEC/IEEE 42010 “Systems and software engineering – Architecture description”. It falls under Generic Framework Standards type; however, the validation and evaluation process of the proposed framework was not included in this study. Furthermore, both of these studies do not prove and nor evaluate their effectiveness in terms of information security. In addition, they do not prevent or mitigate relevant information security risks, hence they do not follow a specific blockchain standards in term of handling the data securely in a blockchain technology and/or enhanced version of HIPPA in case of the first study.

The study by John and Adrian [23] discusses three key areas that should be covered while developing the standards which are blockchain governance, smart contracts and interoperability between and across blockchains. In terms of blockchain security, the study just briefly covers few aspects within these areas and at a high level which are the data governance, key security, smart contracts vulnerabilities and interoperability related security. The study by Kiran et al. [24] discussed the interoperability as well as the enhancement of information technology controls of the following five areas: information security policies, physical security, key management and cryptography controls, computer operations and logical access controls. In addition, it highlighted six key blockchain areas which are: platform, nodes, development, user, security incidents and asset management, along with its involved risks and respective controls in a high-level overview. However, both studies don’t provide a comprehensive and detailed overview of information security controls related to this technology in terms of the number of security controls covered as well as lack of the detailed information into how to protect information security and to manage involved risks in this technology.

The study by Vincent and Mark [25] highlighted the list of the international and regional Standards Developing Organizations (SDOs) that are currently working into developing blockchain related standards. Also, they highlighted the lack of common terminology with the respect of the blockchain technology. In addition, they proposed a high-level description regarding the three elements that should be covered on the blockchain-based functional architecture. The study by Rafael and Rocco [26] reviewed the existed standards in relation to the decentralized cloud solutions and highlighted the relevant general requirements. However, both studies don't highlight and provide any details about the security requirements for the blockchain technology.

Lastly, the study by James and Maria [27] evaluated four major blockchain platforms in term of their compliance with NIST cryptographic standards as per FISMA requirements based on a preselected criteria. Thus, this is ensuring that the relevant cryptographic algorithms are secure from security flaws and vulnerabilities. However, this study covered comprehensively only one domain of the security aspects in relation to the blockchain technology.

Therefore, this thesis aims to cover the limitations of the aforementioned reviews by establishing new information security controls specifically related to the blockchain technology that have been not covered by International and National Information Security Standards which are ISO 27001 and UAE IA Standards.

Chapter 4: Establishing Blockchain Security Controls

To achieve the objective of this thesis, the information security controls especially for the blockchain technology have been firstly established based on the understanding of the technology itself and its involved risks, threats, weaknesses and vulnerabilities in term of information security. The proposed security controls are new and not covered by International and National Information Security Standards which are ISO 27001 & UAE IA Standards. The control structure of these security controls followed the ISO 27002's control structure which includes: control's statement, implementation guidance of control's requirements in detail, and provision further information as well in case of any legal, regulatory and other considerations that should be taken into account (if applicable and/or available).

Table 1 shows the security controls that are related to the blockchain technology specifically including the newly established security controls and already existed and applicable security controls from ISO27001 controls and UAE IA security controls. Theses controls are considered sub controls fall under the following family controls. Figure 3 shows the relevant family controls and their sub controls.

i. Blockchain Governance
ii. Risk Management
iii. Data Management
iv. Identity and Access Management
v. Key and Certificate Management
vi. Network Management
vii. Vulnerability Management
viii. Incident Response
ix. Monitoring and Evaluation

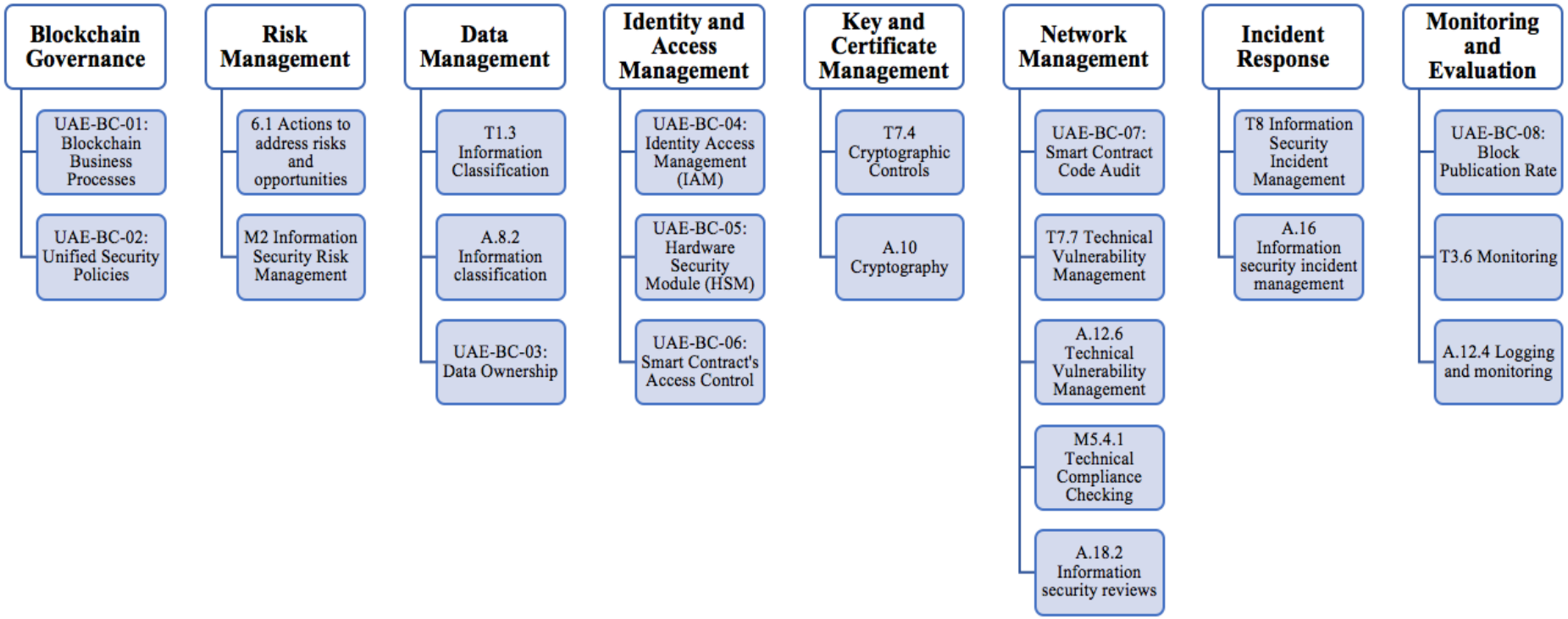


Figure 3: Blockchain Security Family Controls and their Sub Controls

Table 1: Blockchain's Security Controls

Blockchain's Security Controls	Relevant Proposed Security Controls	Relevant Security Controls from UAE IA Standards	Relevant Security Controls from ISO27001 Standard
Family Control: Blockchain Governance Objective: To provide management direction, support and guidance for maintaining the security of the blockchain-based solution.			
The entity shall define and establish a business process and/or procedure in relation of the blockchain solution and its use cases.	UAE-BC-01: Blockchain Business Processes	-	-
All participated entities on permissioned blockchain shall define, document, implement, agreed and follow unified security policies in relation to blockchain-based service.	UAE-BC-02: Unified Security Policies	-	-
Family Control: Risk Management Objective: To maintain the overall security of the blockchain-based solution through identifying, assessing and treating the associated risks that could have an impact on the organization's business processes, people and technology.			
The entity should perform the risk management strategy in relation with blockchain-based solution including but not limited to performing risk assessment and treatment along with on-going monitoring and review.	-	6.1 Actions to Address Risks and Opportunities	M2 Information Security Risk Management

Table 1: Blockchain's Security Controls (Continued)

Blockchain's Security Controls	Relevant Proposed Security Controls	Relevant Security Controls from UAE IA Standards	Relevant Security Controls from ISO27001 Standard
Family Control: Data Management Objective: To maintain the confidentiality, integrity and availability of the data through its lifecycle starting from the data's creation, processing, transferring, exchanging, storing and until the destruction.			
The entity should define, develop, approve and implement a data classification approach/scheme including but not limited to the relevant information of the blockchain-based service in order to protect the information from unauthorized disclosure, modification and destruction.	-	T1.3 Information Classification	A.8.2 Information Classification
All entities shall establish and agree on a process to define the data type that will be stored on the blockchain along with the data's ownership responsibilities.	UAE-BC-03: Data Ownership	-	-

Table 1: Blockchain's Security Controls (Continued)

Blockchain's Security Controls	Relevant Proposed Security Controls	Relevant Security Controls from UAE IA Standards	Relevant Security Controls from ISO27001 Standard
Family Control: Identity and Access Management Objective: To ensure the identity-related services associated with the blockchain-based solution and its relevant applications are provided in a proper and secure manner.			
The entity shall define, design, plan, and implement an Identity Access Management (IAM) solution for the permissioned blockchain-based service in line with the user on-boarding and off-boarding processes.	UAE-BC-04: Identity Access Management (IAM)	-	-
All the entities shall establish and agree on the architecture and procedure for Hardware Security Module (HSM) implementation for securing blockchain identity keys.	UAE-BC-05: Hardware Security Module (HSM)	-	-
Access to smart contract lifecycle management should be defined, controlled, logged and monitored on a continuous basis, including the relevant processes and/or applications that the smart contract will be collaborating with.	UAE-BC-06: Smart Contract's Access Control	-	-

Table 1: Blockchain's Security Controls (Continued)

Blockchain's Security Controls	Relevant Proposed Security Controls	Relevant Security Controls from UAE IA Standards	Relevant Security Controls from ISO27001 Standard
Family Control: Key and Certificate Management Objective: To maintain the confidentiality, integrity and authenticity of the information and/or the applicable services.			
The entity should use strong cryptographic key and certificate management including but not limited to internal and external TLS certificates, identity keys and domain certificates.	-	T7.4 Cryptographic Controls	A.10 Cryptography
Family Control: Network Management Objective: To protect and secure the blockchain-based solution physically and logically along with its relevant underlying infrastructure and communications components.			
The entity should protect and secure the internal and external communications of the blockchain-based solution via using a highly secure channel(s).	-	T4 Communications	A.13 Communications Security
The entity should protect the underlying infrastructure of the blockchain-based solution including but not limited to the physical and logical components.	-	T2 Physical and Environmental Security T5 Access Control	A.11 Physical and Environmental Security A.9 Access Control

Table 1: Blockchain's Security Controls (Continued)

Blockchain's Security Controls	Relevant Proposed Security Controls	Relevant Security Controls from UAE IA Standards	Relevant Security Controls from ISO27001 Standard
Family Control: Vulnerability Management Objective: To protect the blockchain-based solution and its applications and software securely against the threats, vulnerabilities, weaknesses and holes.			
The entity shall establish a process for testing, analyzing and auditing the smart contract code by an independent outsourced specialized party.	UAE-BC-07: Smart Contract Code Audit	-	-
The entity should protect and secure the relevant application programs and/or software of the blockchain-based solution from threats and vulnerabilities.	-	T7.7 Technical Vulnerability Management	A.12.6 Technical Vulnerability Management
The entity should perform full scope vulnerability assessment and penetration testing on the proposed blockchain-based solution.	-	M5.4.1 Technical Compliance Checking	A.18.2 Information Security Reviews
Family Control: Incident Response Objective: To ensure the proper and effective response with the respect to the relevant security incidents.			
The entity should define, develop, implement the security incident and event management process and/or procedure in relation to the blockchain-based solution including preparation, detection and analysis, containment, eradication, and recovery.	-	T8 Information Security Incident Management	A.16 Information Security Incident Management

Table 1: Blockchain's Security Controls (Continued)

Blockchain's Security Controls	Relevant Proposed Security Controls	Relevant Security Controls from UAE IA Standards	Relevant Security Controls from ISO27001 Standard
Family Control: Monitoring and Evaluation Objective: To ensure the continual improvement of the blockchain-based solution through regular and consistent monitoring and evaluation.			
The entity shall establish a process and/or procedure for testing, monitoring and evaluating the publication rate of a block and accordingly adjust influencing factors of the respective rate (if required).	UAE-BC-08: Block Publication Rate	-	-
The entity should continuously monitor blockchain-based solution and its architecture components, applications, software, communications and connection links, the data and its flow and etc.	-	T3.6 Monitoring	A.12.4 Logging and Monitoring
The entity should regularly measure the effectiveness of the implemented security controls related to the blockchain-based solution via, such as but not limited to, performing security controls assessment, auditing the relevant business processes and/or procedures and etc.	-	M6 Performance Evaluation and Improvement	A.18.2 Information Security Reviews

4.1 Proposed Blockchain Security Controls

The following are including the objective of each proposed security controls related to the blockchain technology and the detailed implementation guidance of each one of them.

- UAE-BC-01: Blockchain Business Processes

Objective: To provide clear and comprehensive vision in relation to the business processes and procedures of blockchain-based service and its use cases in order to maintain the business workflow properly and the overall security.

UAE-BC-01: Blockchain Business Processes

Control

The entity shall define and establish a business process and/or procedure in relation of the blockchain solution and its use cases.

Implementation guidance

The defined process and/or procedure should be aligned with the respective operation model and should include, but not limited to, the following considerations:

a. Determine the type of the blockchain-based service, address space and cryptographic functions in use.
b. The signing and/or verifying mechanisms of the transactions, for example the consensus model in use.
c. The mechanism of publishing and adding new blocks on the network including but not limited to the target average publish time along with the relevant incentives (if applicable).

d. Determine the block component taking into considerations the maximum size of the block, transaction and data.
e. Identify all participating entities and their roles within the blockchain-based service in case of a permissioned blockchain.
f. Establish a secure development processes and/or procedure in relation with the smart contracts including but not limited to defining the relevant business requirements and scope of work, using the relevant pre-approved tools and software and reviewing and testing the code on regular basis and prior the deployment.

- UAE-BC-02: Unified Security Policies

Objective: To ensure and maintain the consistency between all participated entities on the respective blockchain platform through implement and follow unified security policies related to designing, developing and using the respective platform.

UAE-BC-02: Unified Security Policies

Control

All participated entities on permissioned blockchain shall define, document, implement, agreed and follow unified security policies in relation to blockchain-based service.

Implementation guidance

All entities should agree on the relevant security policies, standards, and best practices in relation to blockchains to follow and comply with.

The unified security policies shall include, but not limited to, Access Control Policy, Cryptography Policy, Network and Communication Security Policy. Establish and maintain the relevant documentations such as but not limited to processes, procedures, templates, records, plans, logs and/or guidelines. The unified security policies shall be communicated to all users of the participating entities on the blockchain platform. The unified security policies shall be reviewed at planned intervals or in case a significant change occurs on the relevant blockchain-based service and accordingly they shall be updated and approved by all participating entities. <u>Other information</u> Generally, information security policies-based security control has been mentioned on the international and national information security standards, such as but not limited to, the relevant security control number A.5 in ISO/IEC 27001 and M1.2 in UAE Information Assurance Standards.

- UAE-BC-03: Data Ownership

Objective: To define the data type that will be stored on the respective blockchain platform taking into considerations the applicable national and international laws and regulations. In addition, to define the data ownership and the respective roles and responsibilities into handling the relevant data securely.

UAE-BC-03: Data Ownership

Control

All entities shall establish and agree on a process to define the data type that will be stored on the blockchain along with the data's ownership responsibilities.

Implementation guidance

Define the respective roles and responsibilities in relation to the data over the blockchain-based service.

Establish and maintain the relevant documentations on data handling process, including but not limited to the following considerations:

a. The data should be secured during creation, receipt, storage, processing, transmission, disposal and etc.
b. Define data type taking into considerations personal data types as defined by established international standards/regulations such as General Data Protection Regulation (GDPR) and ISO/IEC 27001.
c. Encrypt the data stored on the blockchain using a strong encryption algorithm approved by international and national authorities, such as but not limited to, Abu Dhabi Digital Authority (ADDA) in United Arab Emirates.
d. Verification if the data is correct as required by defined data type, encoding and/or encryption mechanisms.
e. Access criteria on how the data record and/or individual fields of the data record can be retrieved and decrypted.
f. Control the flow of information within the blockchain and between interconnected systems and provide the respective authorizations based on specified service access requirements.

g. The relevant documentations of the processes should include such as but not limited to template, records, plans, audit logs and/or guidelines.

Other information

The General Data Protection Regulation (GDPR) is a data protection and privacy law in the European Union. Since the data stored on the blockchain is immutable, therefore ensuring that the stored data type is not a personal information in order to be comply with the GDPR.

In addition, ISO/IEC 27001 is international standard that is focused on information security and managing its associated risks through Information Security Management System (ISMS) framework.

- UAE-BC-04: Identity Access Management (IAM)

Objective: To identify, authenticate and authorize individuals properly and securely in order to ensure that the proper user have the appropriate access to the respective blockchain platform and its components based on a defined processes and procedures specifically to blockchain-based service and solution.

UAE-BC-04: Identity Access Management (IAM)

Control

The entity shall define, design, plan, and implement an Identity Access Management (IAM) solution for the permissioned blockchain-based service in line with the user on-boarding and off-boarding processes.

Implementation guidance

Define the roles and responsibilities of the identity providers and service providers and accordingly grant the respective permissions and/or privileges.

Maintain and update the list of the identity providers and service providers regularly.

Define and establish user on-boarding and off-boarding processes including the relevant authentication, verification, and authorization mechanisms.

Assign, reassign, validate and/or remove privileges for the users as per the business needs.

Define and establish the blockchain-based service's access process and/or procedures in line with the relevant Access Control Policy; including the access means, such as but not limited to, remote access, wireless access and/or through mobile devices.

Establish and maintain the relevant documentations of the processes such as but not limited to template, records, plans, audit logs and/or guidelines.

The blockchain-based service's access should cover at least the following privileges in line with the least privilege principle:

a. Read access to the blockchain.
b. Publish new transactions to the blockchain.

The relevant account/identity is created, approved, enabled, modified, disabled and removed as per Access Control Policy in relation to blockchain.

Access control can further be restricted to user identity or credential to provide privacy of the transaction content.

Periodically review the relevant account/identity along with its granted/assigned permissions/privileges and the access audits logs/reports as well.

Continuously monitoring, oversighting and auditing user access to the blockchain-based service.

In case of any access violations and/or malicious transaction, release the incident report in line with the approved Information Security Incident Management Policy.

Other information

Generally, access control-based security control has been mentioned on the international and national information security standards, such as but not limited to, the relevant security control number A.9 in ISO/IEC 27001 and T5 in UAE Information Assurance Standards.

- UAE-BC-05: Hardware Security Module (HSM)

Objective: To store, manage and maintain the user private keys securely within the Hardware Security Module (HSM) integrated into the respective blockchain platform in order to ensure its security from being losing, hacking and stealing by a malicious party.

UAE-BC-05: Hardware Security Module (HSM)

Control

All the entities shall establish and agree on the architecture and procedure for Hardware Security Module (HSM) implementation for securing blockchain identity keys.

Implementation guidance

Conduct risk assessment on HSM implementation over the proposed blockchain architecture.

Define and establish HSM partition process for storing the keys along with the respective separated admin rights and roles for each participating entity, such as but not limited to, crypto officer, crypto user and super admin.

Establish and maintain the relevant documentations of the processes such as but not limited to template, records, plans, audit logs and/or guidelines.

Access to the keys should be enabled only through a secure manner.

Other information

Generally, user credentials-based security control has been mentioned on the international and national information security standards, such as but not limited to, the relevant security control number A9.2.4 in ISO/IEC 27001 and T5.2.3 in UAE Information Assurance Standards.

- UAE-BC-06: Smart Contract's Access Control

Objective: To ensure the smart contract code is accessed in a proper and secure manner during its lifecycle as per predefined privileges to respective users. In addition, to ensure that the access to smart code is logged and monitored continuously in order to prevent any malicious activities.

UAE-BC-06: Smart Contract's Access Control

Control

Access to smart contract lifecycle management should be defined, controlled, logged and monitored on a continuous basis, including the relevant processes and/or applications that the smart contract will be collaborating with.

Implementation guidance

Define the user's role and responsibilities in regard to smart contract 's access along with predefined and approved access control list.

Ensure the segregation of duties.

Establish a process/procedure for defining, controlling and monitoring the access to the smart contract through its lifecycle including other interactions with relevant processes and/or applications.

Establish and maintain the relevant documentations of the process and/or procedure such as but not limited to template, records, plans, logs and/or guidelines.

Use cryptographic solutions such as but not limited to Trusted Platform Modules (TPMs) for sensitive code execution.

Payment and time list for smart contract execution to be clarified for given blockchain services to ensure denial of service attacks on the publishing node (e.g. full system resource consumption) are prevented.

In case of any access violations and/or malicious transactions, release the incident report in line with the approved Information Security Incident Management Policy.

Other information

Generally, access control-based security control has been mentioned on the international and national information security standards, such as but not limited to, the relevant security control number A.9 in ISO/IEC 27001 and T5 in UAE Information Assurance Standards.

- UAE-BC-07: Smart Contract Code Audit

Objective: To ensure the smart contract code is tested and audited prior its deployment in order to be secured and protected against the security vulnerabilities,

bugs and flaws thus prevent any malicious activities that could negatively effect on the security of the respective blockchain platform.

UAE-BC-07: Smart Contract Code Audit

Control

The entity shall establish a process for testing, analyzing and auditing the smart contract code by an independent outsourced specialized party.

Implementation guidance

Establish and maintain the relevant documentations of the relevant process and/or procedure such as but not limited to template, records, plans, logs and/or guidelines.

The need to comprehend business logic of the smart contract to validate that the code is compliant with the service need.

The smart contract should be tested and audited against legal considerations, security vulnerabilities, bugs and flaws by independent party.

The smart contract should be analyzed using for example, but not limited to, Expert code Analysis, Control Flow Analysis, Dynamic Code Analysis, Manual Code Analysis, Vulnerability-based Analysis, Taint Analysis, Symbolic Execution and Improper Error Handling.

The smart contract should be published on the blockchain-based service based on the outcomes of the relevant testing, auditing and analysis reports along with the respective approval from the process owner.

Ensure that the smart contract execution is not relying on predefined timestamps for determining whether or not to take an action such as making a payment in order to avoid malicious activities such as propagation delay, synchronization errors, etc.

Other information

Generally, information system audit-based security control has been mentioned on the international and national information security standards, such as but not limited to, the relevant security control number A.12.7 in ISO/IEC 27001 and M5.5 in UAE Information Assurance Standards.

- UAE-BC-08: Block Publication Rate

Objective: To ensure and maintain the overall security of the respective blockchain platform and prevent any malicious activities on the block production process through performing a proper testing, monitoring and evaluation techniques.

UAE-BC-08: Block Publication Rate

Control

The entity shall establish a process and/or procedure for testing, monitoring and evaluating the publication rate of a block and accordingly adjust influencing factors of the respective rate (if required).

Implementation guidance

The defined process and/or procedure should include, but not limited to, the following considerations:

a. Agreement on block's validation process of the blockchain-based service. This determines selection criteria of the validators.
b. Mechanism on how such new blocks are published to all nodes.
c. Details on mathematical calculation adjustment to match changes in computational capacity of blockchain network to meet a specified average

time for successful mining of a single block in case of permissionless blockchain.

d. Regularly testing and monitoring the effectiveness of the block publication rate against the malicious activities as per the established plans.
e. Adjust the block publication rate according to the outcomes of the relevant testing, monitoring and evaluation reports along with the respective approval from the process owner.
f. Establish and maintain the relevant documentations of the respective process and/or procedure such as but not limited to template, records, plans, logs and/or guidelines.

4.2 Performing Risk Assessment and Treatment

In order to determine the security controls appropriately, Risk Assessment and Risk Treatment have been performed on five blockchain use cases to determine their involved risks with their respective security controls as per ISO 31000:2018 – Risk Management (See ISO 31000 [28]). Their relevant applications focused on the medical records, student digital documents and energy and financial services.

Therefore, the impact and probability criteria have been defined along with their relevant definition and description as shown on Tables 2 and 3. Accordingly, the risk matrix has been established as shown on Figure 4 along with the relevant risk rating definition and description as shown on Table 4. The risk acceptance criteria have been excluded as it depends on the organization management decision which is out of this research scope.

Table 2: Impact Levels Description

Impact Level	Definition
Very High	The threat event could be expected to have multiple severe or catastrophic adverse impact on the organization's people, process, and/or technology, or the nation.
High	The threat event could be expected to have a severe or catastrophic adverse impact on the organization's people, process, and/or technology, or the nation.
Medium	The threat event could be expected to have a serious adverse impact on the organization's people, process, and/or technology.
Low	The threat event could be expected to have a limited adverse impact on the organization's people, process, and/or technology.

Table 3: Probability Levels Description

Probability Level	Definition
Very High	A threat event is almost certain to occur, or occurs more than 100 times a year.
High	A threat event is highly likely to occur, or occurs between 1-100 times a year.
Medium	A threat event is moderately likely to occur, or occurs between 1-10 times a year.
Low	A threat event is unlikely to occur, or occurs less than once a year, but more than once every 10 years.

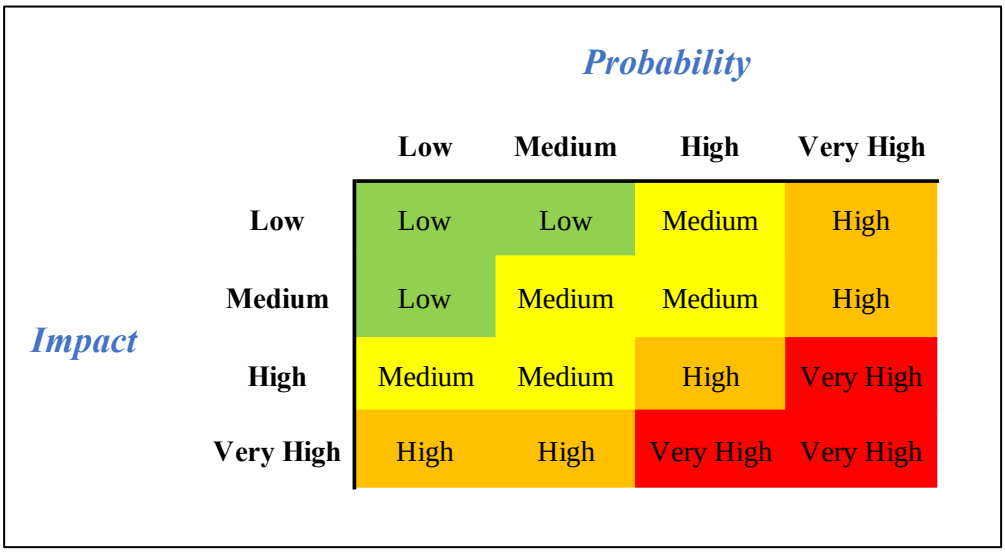


Figure 4: Risk Matrix

Table 4: Risk Rating Description

Risk Rating	Definition
Very High	If a risk is rated as "Very High", there is an immediate requirement for mitigation actions. The affected information asset should be assessed for possible impact and a risk mitigation action must be planned, agreed, and implemented before continuing its operation, within the agreed period of time.
High	If a risk is rated as "High", there is an urgent requirement for mitigation actions. The affected information asset may continue to operate with compensating controls, but a risk mitigation action must be planned, agreed, and implemented, within the agreed period of time.
Medium	If a risk is rated as "Medium", a mitigation action is required, and a plan must be developed to incorporate these actions and implemented within an agreed period of time.
Low	If a risk is rated as "Low", then the organization may decide to implement a mitigation action or to accept the risk.

The Risk Assessment and Treatment have been performed on the chosen blockchain use cases as the following:

1. Risk Assessment

Risk Assessment consists of Risk Identification, Risk Analysis and Risk Evaluation.

1.1 Risk Identification

The involved risks, threats and vulnerabilities of the blockchain use cases (along with their services, systems, etc.) have been identified with respect to information security through different techniques and methods including, interviewing owners and respective people related to blockchain use cases and viewing the relevant documents. Therefore, a comprehensive list of the identified risks has been prepared, as part of this stage.

1.2 Risk Analysis

The identified risks have been analyzed by first identifying its sources and its potential incident scenarios, along with determining the probability as well as the impact for each incident scenarios based on the established probability criteria and impact criteria sequentially. The risk value for each incident scenarios is calculated by multiplying the determined probability value with the determined impact value.

1.3 Risk Evaluation

The determined and calculated risk value on the Risk Analysis is considered as an input for Risk Evaluation. The risk value on the established risk matrix is the corresponding value of the determined probability value and the determined impact value of each incident scenario.

2. Risk Treatment

Risk Treatment has been performed to treat the identified risks. Generally, there are four options for treating risks which are:

a. Risk Reduction: Mitigating the risks through applying the appropriate security controls.
b. Risk Retention/Acceptance: Accepting the risks that falls within the defined risk acceptance level.
c. Risk Avoidance: Avoiding the tasks and/or activities that cause a risk.
d. Risk Transfer: Transferring the risk to another party.

As per the aim of this research, the primary option in this stage is Risk Reduction. Accordingly, the appropriate security controls have been selected from UAE IA Standard's controls, ISO 27001 Standard's controls and the proposed security controls. The Risk Avoidance option has been not used since there is no particular process or activity to avoid it. Regarding the remaining options, the Risk Retention/Acceptance and Risk Transfer, they are dependent on the risk owner and/or organization management decision therefore they are out this research scope.

4.2.1 Blockchain Use Cases

- Use Case#1 – MedRec – MIT

Since patients are moving between different health service providers, their data becomes scattered; each provider keeps the patient health records under its supervision which can leads in the patient being unable to view their health information and reports, correct any error data and distribute their information across the health providers. Therefore, MedRec is a proposal that aims to solve this issue through

eliminating the centralization and providing the transparent access to the health records by using blockchain technology. Moreover, it is a distributed system that provides access and validation features to patient health records from different providers. It is a private Ethereum based blockchain platform. It does not store the patient records on the MedRec blockchain platform; rather it use smart contract to encode the data of the relevant record locations that links to the actual records which stored off chain which can be retrieved by using database queries thus can be accessed securely by the respective patient and different providers. In addition, the relationship between the patient and the respective providers is added using the smart contract including the respective permissions. Figure 5 shows MedRec Architecture.

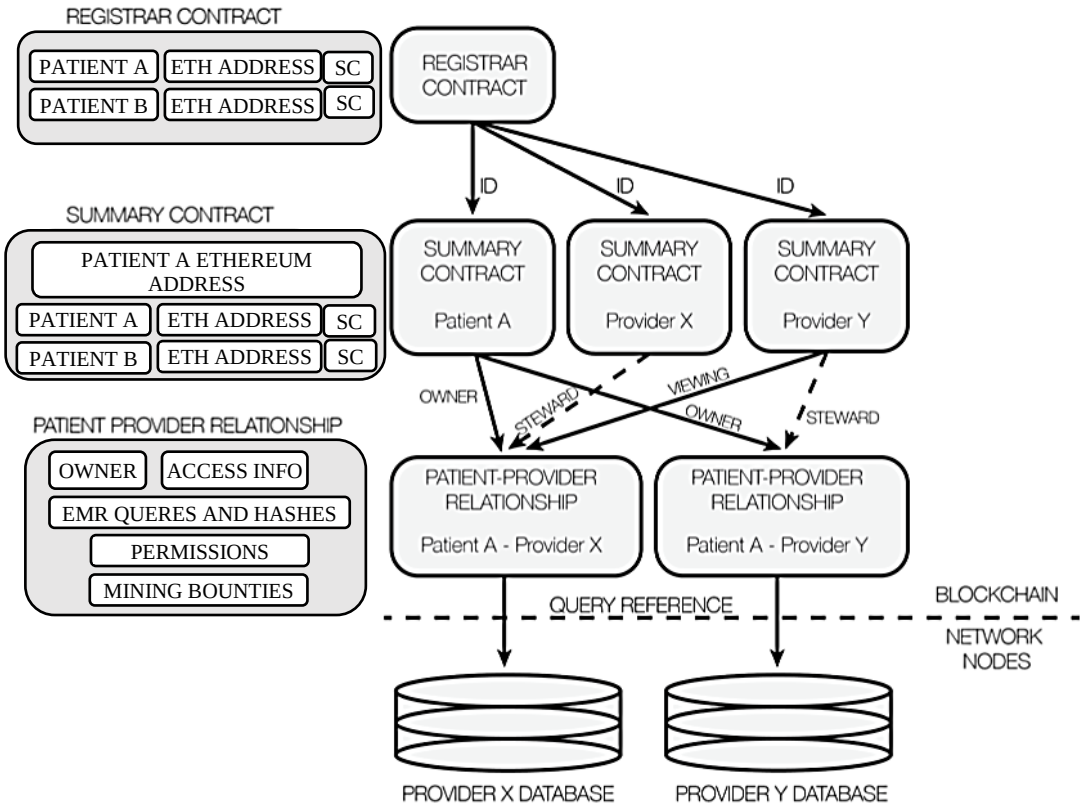


Figure 5: MedRec Architecture (Source: [29])

More detailed information about the MedRec can be find in their technical document [29].

- Use Case#2 – Energy Web

The decentralization property of the blockchain technology has helped into the utility investment through the renewable energy generation, transmission, and distribution. Therefore, Energy Web Decentralized Operating System (EW-DOS) aims to use the decentralized digital technologies to accelerate the global transition into a low carbon energy future life. Moreover, it is a public based blockchain network for energy trading and tracking between the customers, service providers, retailers and grid operators. Thus, anyone can access the network, deploy smart contract and build, develop and deploy any app on the respective network through paying a token (Energy Web Token "EWT") for the relevant services and/or transactions. It uses Proof of Authority (PoA) model. A "transaction relay server" is used for ensuring that all transactions are mined and are error free. It uses also a self-sovereign decentralized digital identity (DIDs) with multi-signature wallet which provide the user the ability to control over its personal information usage and management. The respective node categories into 2 types, one is validator node and the another is utility node. In case an organization will host both node types, then it required to configure a specific container "Docker images" on the respective host. In addition, it uses Application Programming Interfaces (API)s for interacting and transferring the data between blockchain platform and other external components and/or platforms. Figure 6 shows the interrelated layers of the respective platform which are Trust, Utility and Toolkit, and their components.

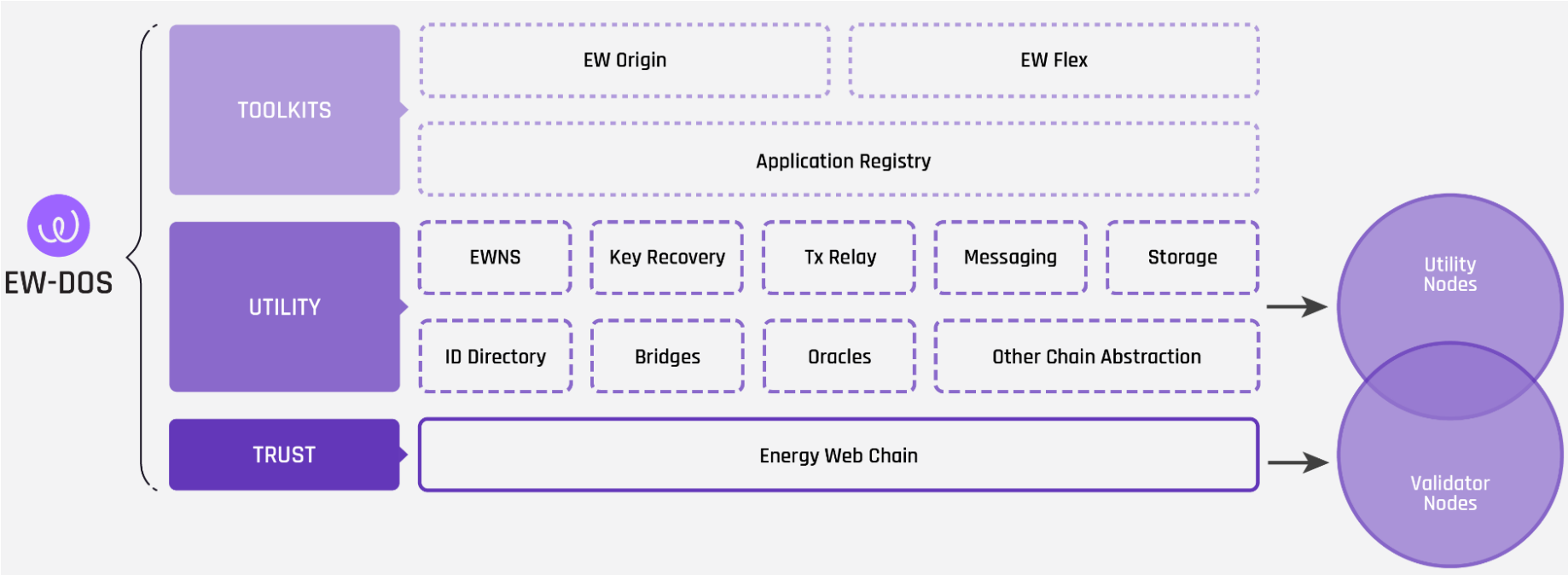


Figure 6: EW-DOS Layers (Source: [30])

More detailed information about this solution can be find in their technical document [30].

- Use Case#3 – Power Ledger

Power Ledger is renewable energy trading platform that uses blockchain technology to facilitate the financial settlement and reconciliation of the energy transactions between the participating parties in higher speed and at the same intervals in which the energy is produced and consumed without the need of a central authority. It is a hybrid public and consortium based blockchain platform. It supports a number of energy trading applications. Also, it uses smart contract. One of its native tokens called POWER token; which is mainly used for facilitating and providing access permission to the respective platform. Thus, it is considered as an access token. The utility company which represents as an application host is responsible for managing and on-boarding participants on the respective platform. It uses APIs for gathering the required information between external components and blockchain layers that one is public and the other is consortium blockchains which called “EcoChain”; it is a private based blockchain that uses Proof of Stake (PoS) model. The state channels are used to handle high frequency energy transaction settlements in an off-chain manner. Figure 7 shows the Power Ledger layers and its components.

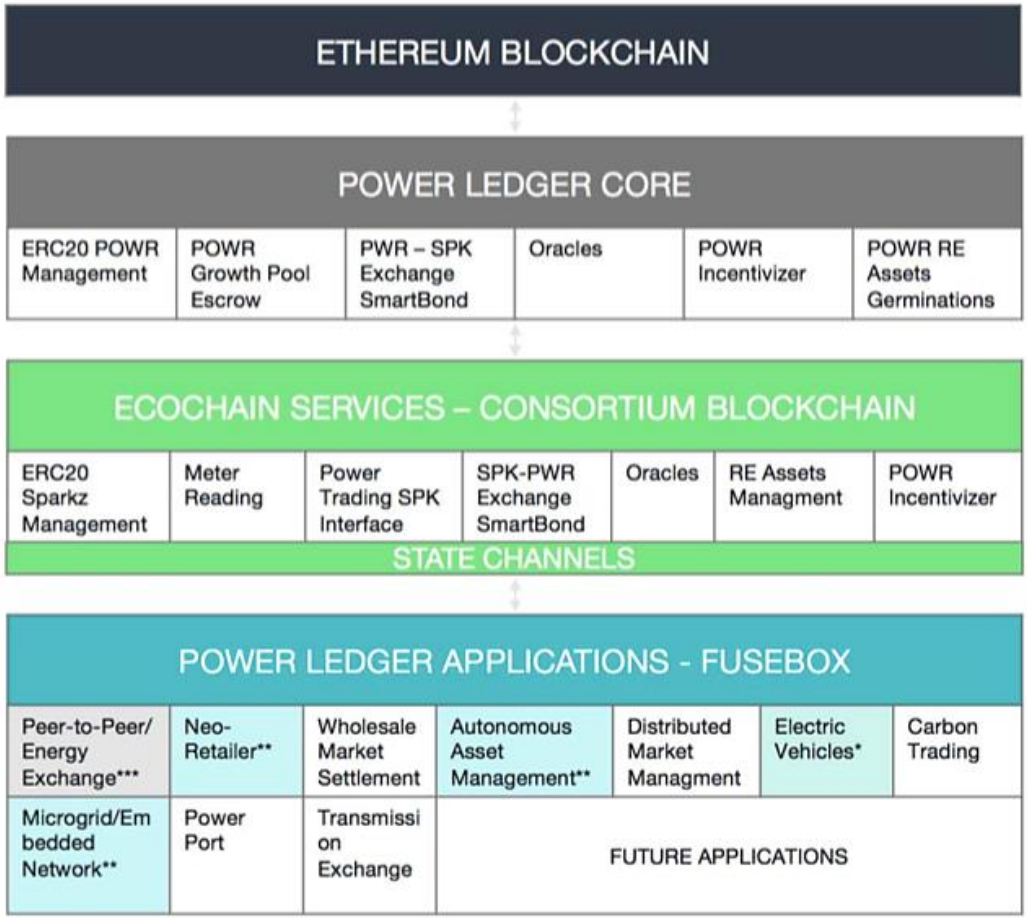


Figure 7: Power Ledger layers and its components (Source: [31])

Regarding this solution, a high-level technical detail only is available. However, more general information about it can be find in their paper [31].

- Use Case#4 – Confidential

It is a digital wallet which holds the digital academic records related to the students and alumni on the respective platform. It uses blockchain technology for a smarter digital transformation with the respect to the academic records. It enables all students and alumni to manage and share their academic records in a secure, efficient and flexible ways. Moreover, it enables the respective user to request, manage and share their document with the other entities (for example, applying for job applications). In addition, the respective entities can also verify the provided

documents by the user through using the respective platform. It is fully integrated with the existing IT systems owned by respective organization.

- Use Case#5 – Provenance

Global financial markets invest billions of dollars yearly in the financial services including, such as but not limited to, the audit, custody, trustee, reconciliation and administration services. However, these markets is suffering from limited liquidity, significant friction, lack of transparency. Therefore, Provenance uses blockchain technology in order to reduce the relevant costs and risk, improve liquidity and open new financial markets through providing the financial services via registering and exchanging financial assets across markets such as the loan origination and servicing and securitization. It is public but permissioned based blockchain platform. It uses Proof of Stake (PoS) consensus model. In addition, it uses smart contracts. It uses native digital token called Hash. Its respective members categories into four types which are the administrator, member, bank and stakeholder. The administrator is responsible for allocating permissions for the respective member, monitoring them, approving and setting stakes, writing and reviewing smart contracts. There is a lack of technical details about this solution. However, more general information about it can be find in their whitepaper [32].

4.2.2 Risks Registers of Blockchain Use Cases

Tables 5 to 9 shows the risk register of different use cases such as medrec – MIT, energy web, power ledger, confidential and provenance.

Table 5: Risk Register of Use Case#1 – MedRec – MIT

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-01	Lack of enforcement for strong security access controls on the patient's and provider's nodes to prevent unauthorized access to the respective private key.	- User credentials - Respective platform and its components	Medium	Very High	**High**	A.9 Access Control	T5 Access Control	UAE-BC-05: Hardware Security Module (HSM)
R-02	No specified mechanism to protect node's private key from loss.	- User credentials - Respective platform and its components	Medium	Very High	**High**	A9.2.4 Management of Secret Authentication Information of Users	T5.2.3 User Security Credentials Management	UAE-BC-05: Hardware Security Module (HSM)
R-03	No specified mechanism for the node's revocation.	- Abuse the respective platform and its components	Low	Medium	**Low**	A.9.2.1 User Registration and De-Registration A.9.2.2 User Access Provisioning A.9.2.6 Removal or Adjustment of Access Rights	M4.4.3 Removal of Access Rights T5.2.3 User Security Credentials Management	UAE-BC-04: Identity Access Management (IAM)

Table 5: Risk Register of Use Case#1 – MedRec – MIT (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-04	Lack of the endpoint/node's security along with its relevant applications and software from relevant security threats and vulnerabilities.	- Node - User credentials - Respective platform and its components	Medium	Very High	**High**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-
R-05	Lack of multi-authentication mechanisms for accessing the relevant databases.	- Database - Patient data - Respective platform and its components	Low	Medium	**Low**	A9.2 User Access Management	T5.2 User Access Management	-
R-06	Lack of enforcement for database encryption on both the patient's and provider's nodes in order to prevent data leakage and unauthorized disclosure, modification and/or destruction.	- Database - Patient data - Respective platform and its components	Medium	Very High	**High**	A.10 Cryptography	T7.4 Cryptographic Controls	UAE-BC-03: Data Ownership
R-07	Lack of database query protection against relevant well known security vulnerabilities.	- Database - Patient data - Respective platform and its components	Medium	High	**Medium**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-

Table 5: Risk Register of Use Case#1 – MedRec – MIT (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-08	Absence of the monitoring strategy for the respective platform.	- Respective platform and its components and nodes	High	Very High	**Very High**	T3.6 Monitoring M6 Performance Evaluation and Improvement	A.12.4 Logging and monitoring A.18.2 Information security reviews	UAE-BC-08: Block Publication Rate
R-09	Untested and unaudited smart contracts from the relevant security threats and vulnerabilities prior the deployment.	- Respective smart contract - Respective nodes - Respective platform and its components	Medium	High	**Medium**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	UAE-BC-07: Smart Contract Code Audit
R-10	Unauthorized access to the smart contract.	- Respective smart contract - Respective nodes - Respective platform and its components	Medium	High	**Medium**	A.9 Access Control	T5 Access Control	UAE-BC-06: Smart Contract's Access Control
R-11	Unclear vision on the used consensus mechanism for signing, verifying and publishing the block on the respective platform.	- Block production - Business processes	Low	Medium	**Low**	-	-	UAE-BC-01: Blockchain Business Processes

Table 5: Risk Register of Use Case#1 – MedRec – MIT (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-12	Unspecified requirements for secure communication over the platform and its components.	- Respective platform and its network, applications and nodes components	Medium	High	**Medium**	A.13 Communications Security A.11 Physical and Environmental Security A.9 Access Control	T4 Communications T2 Physical and Environmental Security T5 Access Control	-
R-13	Incidents reporting procedure is not specified.	- Respective platform and its network, applications and nodes components	Medium	High	**Medium**	A.16 Information Security Incident Management	T8 Information Security Incident Management	-
R-14	Unclear vision with respect to data security and confidentiality including but not limited to the block payloads, transmitted data and data at rest.	- Data	Medium	Very High	**High**	A.10 Cryptography	T7.4 Cryptographic Controls	UAE-BC-03: Data Ownership
R-15	Unclear vision on the data type that will be stored on the blockchain platform.	- Data	Medium	Very High	**High**	-	-	UAE-BC-03: Data Ownership
R-16	Absence of business continuity strategy for the respective platform.	- Respective platform	Medium	Very High	**High**	A.17 Information Security Aspects of Business Continuity Management	T9 Information Systems Continuity Management	-

Table 5: Risk Register of Use Case#1 – MedRec – MIT (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-17	Lack of the details with the respect to the security of the used cryptographic algorithm against security flaws and vulnerabilities.	- Data - The chain of the blocks	Low	High	**Medium**	A.10 Cryptography	T7.4 Cryptographic Controls	-
R-18	Lack of protection against possible malicious activities of administrators.	- Abuse of privileges - Respective platform and its network, applications and nodes components	Medium	High	**Medium**	A.12.4.3 Administrator and Operator Logs	T3.6.3 Monitoring System Use T3.6.5 Administrator and Operator Logs T5.2.2 Privileges Management	-

Table 6: Risk Register of Use Case#2 – Energy Web

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-01	Lack of vision whether the required security assessment against the relevant security threats and vulnerabilities has been performed on the toolkits before the deployment.	- Respective toolkit - Respective platform and its components	Medium	High	**Medium**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-
R-02	Failure to specify and embed the necessary security requirements for the developers to adhere while they are developing and building the relevant solutions, tools and back-end application services on the respective platform.	- Respective platform and its applications, tools and services components	Medium	Medium	**Medium**	A.14.1 Security Requirements of Information Systems A.12 Operation Security	M5.4 Compliance with Technical Requirements T3 Operations Management	-
R-03	Lack of enforcement for performing the required security assessment (such as threat and vulnerability assessment) of the developed solutions, tools and back-end application services before deploying them on the respective platform.	- Respective platform and its applications, tools and services components	Medium	High	**Medium**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-

Table 6: Risk Register of Use Case#2 – Energy Web (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-04	Lack of the endpoint/node's security along with its relevant applications and software from relevant security threats and vulnerabilities.	- Node - User credentials - Respective platform and its components	Medium	Medium	**Medium**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-
R-05	Lack of security vision on the specified APIs and whether it has been tested against the relevant security threats, vulnerabilities, bugs and holes, and data breaches and DoS attack as well.	- Data - Respective platform and its components	Medium	Very High	**High**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-
R-06	Unclear vision on the data flow within and between the respective platform and its other linked platforms and applications.	- Data	Medium	Very High	**High**	A.13 Communications Security	T4 Communications	-

Table 6: Risk Register of Use Case#2 – Energy Web (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-07	Unclear vision with the respect of the security level of "transaction relay server" including but not limited to physical security, patching and server maintenance, event logs, system integrity control, anti-virus and anti-malware, authentication and access controls, and backups and restore.	- Respective server	Medium	Very High	**High**	A.11 Physical and Environmental Security A.12 Operation Security A.14 System Acquisition, Development and Maintenance A.9 Access Control	T2 Physical and Environmental Security T3 Operations Management T7 Information Systems Acquisition, Development and Maintenance T5 Access Control	-
R-08	Untested and unaudited smart contracts from the relevant security threats and vulnerabilities prior the deployment.	- Respective smart contract - Respective nodes - Respective platform and its components	Medium	High	**Medium**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	UAE-BC-07: Smart Contract Code Audit

Table 6: Risk Register of Use Case#2 – Energy Web (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-09	Unauthorized access to the smart contract.	- Respective smart contract - Respective nodes - Respective platform and its components	Low	High	**Medium**	A.9 Access Control	T5 Access Control	UAE-BC-06: Smart Contract's Access Control
R-10	Unclear vision on how the key pair that reside on the respective network are protected against hacking, theft, malicious activities and unauthorized access.	- User credentials - Respective platform and its components	Medium	Very High	**High**	A.9 Access Control A.10 Cryptography	T5 Access Control T7.4 Cryptographic Controls	UAE-BC-05: Hardware Security Module (HSM)
R-11	Unclear vision with respect to data security and confidentiality including but not limited to the block payloads, transmitted data and data at rest.	- Data	Medium	Very High	**High**	A.10 Cryptography	T7.4 Cryptographic Controls	UAE-BC-03: Data Ownership
R-12	Lack of the details with the respect to the security of the used cryptographic algorithm against security flaws and vulnerabilities.	- Data - The chain of the blocks	Low	High	**Medium**	A.10 Cryptography	T7.4 Cryptographic Controls	-
R-13	Unclear vision on the data type that will be stored on the blockchain platform.	- Data	Medium	Very High	**High**	-	-	UAE-BC-03: Data Ownership

Table 6: Risk Register of Use Case#2 – Energy Web (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-14	Lack of protection against possible malicious activities of administrators and/or validators.	- Abuse of privileges - Respective platform and its network, applications and nodes components	Low	High	**Medium**	A.12.4.3 Administrator and Operator Logs	T3.6.3 Monitoring System Use T3.6.5 Administrator and Operator Logs T5.2.2 Privileges Management	-
R-15	Lack of the security requirements enforcement while the developers are configuring the respective Docker images such as but not limited to threat and vulnerability management, patch management and etc.	- Respective docker images - Respective platform and its components	Low	Medium	**Low**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews A.12 Operation Security	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking T3 Operations Management	-

Table 7: Risk Register of Use Case#3 – Power Ledger

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-01	Lack of the endpoint/node's security along with its relevant applications and software from relevant security threats and vulnerabilities.	- Node - User credentials - Respective platform and its components	Medium	Very High	**High**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-
R-02	Lack of security vision on the specified APIs and whether it has been tested against the relevant security threats, vulnerabilities, bugs and holes, and data breaches and DoS attack as well.	- Data - Respective platform and its components	Medium	Very High	**High**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-
R-03	Unclear vision on the data flow within and between the respective platform and its other linked platforms and/or applications.	- Data	Medium	Very High	**High**	A.13 Communications Security	T4 Communications	-
R-04	Unclear vision with respect to data security and confidentiality including but not limited to the block payloads, transmitted data and data at rest.	- Data	Medium	Very High	**High**	A.10 Cryptography	T7.4 Cryptographic Controls	UAE-BC-03: Data Ownership
R-05	Lack of the details with the respect to the security of the used cryptographic algorithm against security flaws and vulnerabilities.	- Data - The chain of the blocks	Low	High	**Medium**	A.10 Cryptography	T7.4 Cryptographic Controls	-

Table 7: Risk Register of Use Case#3 – Power Ledger (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-06	Unclear vision on the data type that will be stored on the blockchain platform.	- Data	Medium	Very High	**High**	-	-	UAE-BC-03: Data Ownership
R-07	Lack of protection against possible malicious activities of administrators.	- Abuse of privileges - Respective platform and its network, applications and nodes components	Medium	High	**Medium**	A.12.4.3 Administrator and Operator Logs	T3.6.3 Monitoring System Use T3.6.5 Administrator and Operator Logs T5.2.2 Privileges Management	-
R-08	Lack of enforcement for strong security access controls for the nodes to prevent unauthorized access to the respective private key.	- User credentials - Respective platform and its components	Medium	Very High	**High**	A.9 Access Control	T5 Access Control	UAE-BC-05: Hardware Security Module (HSM)
R-09	No specified mechanism to protect node's private key from loss.	- User credentials - Respective platform and its components	Medium	Very High	**High**	A9.2.4 Management of Secret Authentication Information of Users	T5.2.3 User Security Credentials Management	UAE-BC-05: Hardware Security Module (HSM)

Table 7: Risk Register of Use Case#3 – Power Ledger (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-10	No specified node's revocation mechanism.	- Abuse the respective platform and its components	Low	Medium	**Low**	A.9.2.1 User Registration and De-Registration A.9.2.2 User Access Provisioning A.9.2.6 Removal or Adjustment of Access Rights	M4.4.3 Removal of Access Rights T5.2.3 User Security Credentials Management	UAE-BC-04: Identity Access Management (IAM)
R-11	Absence of the monitoring strategy for the respective blockchain platform.	- Respective platform and its components and nodes	High	Very High	**Very High**	T3.6 Monitoring M6 Performance Evaluation and Improvement	A.12.4 Logging and Monitoring A.18.2 Information Security Reviews	UAE-BC-08: Block Publication Rate

Table 7: Risk Register of Use Case#3 – Power Ledger (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-12	Untested and unaudited smart contracts from the relevant security threats and vulnerabilities prior the deployment.	- Respective smart contract - Respective nodes - Respective platform and its components	Medium	High	**Medium**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	UAE-BC-07: Smart Contract Code Audit
R-13	Unauthorized access to the smart contract.	- Respective smart contract - Respective nodes - Respective platform and its components	Low	High	**Medium**	A.9 Access Control	T5 Access Control	UAE-BC-06: Smart Contract's Access Control
R-14	Unspecified requirements for secure communication over the platform and its components.	- Respective platform and its network, applications and nodes components	Medium	High	**Medium**	A.13 Communications Security A.11 Physical and Environmental Security A.9 Access Control	T4 Communications T2 Physical and Environmental Security T5 Access Control	-

Table 7: Risk Register of Use Case#3 – Power Ledger (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-15	Incidents reporting procedure is not specified.	- Respective platform and its network, applications and nodes components	Medium	High	**Medium**	A.16 Information Security Incident Management	T8 Information Security Incident Management	-
R-16	Unclear vision with respect to data security and confidentiality including but not limited to the block payloads, transmitted data and data at rest.	- Data	Medium	Very High	**High**	A.10 Cryptography	T7.4 Cryptographic Controls	UAE-BC-03: Data Ownership
R-17	Absence of business continuity strategy for the respective blockchain platform.	- Respective platform	Medium	Very High	**High**	A.17 Information Security Aspects of Business Continuity Management	T9 Information Systems Continuity Management	-
R-18	Lack of the details with the respect to the security of the used cryptographic algorithm against security flaws and vulnerabilities.	- Data - The chain of the blocks	Low	High	**Medium**	A.10 Cryptography	T7.4 Cryptographic Controls	-

Table 8: Risk Register of Use Case#4 – Confidential

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-01	Unclear vision with respect to data security and confidentiality including but not limited to the block payloads, transmitted data and data at rest.	- Data	Medium	Very High	**High**	A.10 Cryptography	T7.4 Cryptographic Controls	UAE-BC-03: Data Ownership
R-02	Lack of the details with the respect to the security of the used cryptographic algorithm against security flaws and vulnerabilities.	- Data - The chain of the blocks	Low	High	**Medium**	A.10 Cryptography	T7.4 Cryptographic Controls	-
R-03	Lack of protection against possible malicious activities of administrators.	- Abuse of privileges - Respective platform and its network, applications and nodes components	Medium	High	**Medium**	A.12.4.3 Administrator and Operator Logs	T3.6.3 Monitoring System Use T3.6.5 Administrator and Operator Logs T5.2.2 Privileges Management	-
R-04	Lack of vision whether the required security assessment against the relevant security threats and vulnerabilities has been performed on the respective platform before the deployment.	- Respective platform and its components	Medium	High	**Medium**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-

Table 8: Risk Register of Use Case#4 – Confidential (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-05	Unspecified requirements for secure communication over the platform and the other components such as the servers and databases.	- Respective platform and its network, applications and nodes components	Medium	High	**Medium**	A.13 Communications Security A.11 Physical and Environmental Security A.9 Access Control	T4 Communications T2 Physical and Environmental Security T5 Access Control	-
R-06	Unclear vision on the data flow within and between the respective platform and its other linked applications, servers and databases.	- Data	High	Very High	**Very High**	A.13 Communications Security	T4 Communications	-
R-07	Unclear vision on the data type that will be stored on the blockchain platform.	- Data	Medium	Very High	**High**	-	-	UAE-BC-03: Data Ownership

Table 9: Risk Register of Use Case#5 – Provenance

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-01	Lack of vision whether the required security assessment against the relevant security threats and vulnerabilities has been performed on the respective platform before the deployment.	- Respective platform and its components	Medium	High	**Medium**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-
R-02	Unclear vision on the data flow within and between the respective platform and its other components.	- Data	High	Very High	**Very High**	A.13 Communications Security	T4 Communications	-
R-03	Unclear vision on the data type that will be stored on the blockchain platform.	- Data	Medium	Very High	**High**	-	-	UAE-BC-03: Data Ownership
R-04	Lack of enforcement for strong security access controls for the node to prevent unauthorized access to the respective private key.	- User credentials - Respective platform and its components	Medium	Very High	**High**	A.9 Access Control	T5 Access Control	UAE-BC-05: Hardware Security Module (HSM)
R-05	No specified mechanism to protect node's private key from loss.	- User credentials - Respective platform and its components	Medium	Very High	**High**	A9.2.4 Management of Secret Authentication Information of Users	T5.2.3 User Security Credentials Management	UAE-BC-05: Hardware Security Module (HSM)

Table 9: Risk Register of Use Case#5 – Provenance (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-06	No specified mechanism for the node's revocation.	- Abuse the respective platform and its components	Low	Medium	**Low**	A.9.2.1 User Registration and De-Registration A.9.2.2 User Access Provisioning A.9.2.6 Removal or Adjustment of Access Rights	M4.4.3 Removal of Access Rights T5.2.3 User Security Credentials Management	UAE-BC-04: Identity Access Management (IAM)
R-07	Lack of the endpoint/node's security along with its relevant applications and software from relevant security threats and vulnerabilities.	- Node - User credentials - Respective platform and its components	Medium	Very High	**High**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-

Table 9: Risk Register of Use Case#5 – Provenance (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-08	Untested and unaudited smart contracts from the relevant security threats and vulnerabilities prior the deployment.	- Respective smart contract - Respective nodes - Respective platform and its components	Medium	High	**Medium**	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	UAE-BC-07: Smart Contract Code Audit
R-09	Unauthorized access to the smart contract.	- Respective smart contract - Respective nodes - Respective platform and its components	Medium	High	**Medium**	A.9 Access Control	T5 Access Control	UAE-BC-06: Smart Contract's Access Control
R-10	Unspecified requirements for secure communication over the platform and its components.	- Respective platform and its network, applications and nodes components	Medium	High	**Medium**	A.13 Communications Security A.11 Physical and Environmental Security A.9 Access Control	T4 Communications T2 Physical and Environmental Security T5 Access Control	-

Table 9: Risk Register of Use Case#5 – Provenance (Continued)

Risk ID	Risk Description	Asset Affected	Probability (P)	Impact (I)	Risk Value (P * I)	Recommended Security Controls		
						ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-11	Incidents reporting procedure is not specified.	- Respective platform and its network, applications and nodes components	Medium	High	**Medium**	A.16 Information Security Incident Management	T8 Information Security Incident Management	-
R-12	Unclear vision with respect to data security and confidentiality including but not limited to the block payloads, transmitted data and data at rest.	- Data	Medium	Very High	**High**	A.10 Cryptography	T7.4 Cryptographic Controls	UAE-BC-03: Data Ownership
R-13	Lack of the details with the respect to the security of the used cryptographic algorithm against security flaws and vulnerabilities.	- Data - The chain of the blocks	Low	High	**Medium**	A.10 Cryptography	T7.4 Cryptographic Controls	-
R-14	Absence of business continuity strategy for the respective platform.	- Respective platform	Medium	Very High	**High**	A.17 Information Security Aspects of Business Continuity Management	T9 Information Systems Continuity Management	-
R-15	Lack of protection against possible malicious activities of administrators.	- Abuse of privileges - Respective platform and its network, applications and nodes components	Medium	High	**Medium**	A.12.4.3 Administrator and Operator Logs	T3.6.3 Monitoring System Use T3.6.5 Administrator and Operator Logs T5.2.2 Privileges Management	-

Chapter 5: Analysis and Discussion

The performed risk assessment on the relevant blockchain use cases show that like any other technology, blockchain technology beside its benefits can involves some security risks that require some actions to mitigate them and keep pace using the relevant technology. Figure 8 show the associated risks of the relevant use cases which have been categorized as per the risk rating levels. Such that the majority of the associated risks were rated as Medium and High. Therefore, this is proved that there are some moderate/high risks that should be governed and reduce their implications through applying the appropriate security controls including the proposed one.

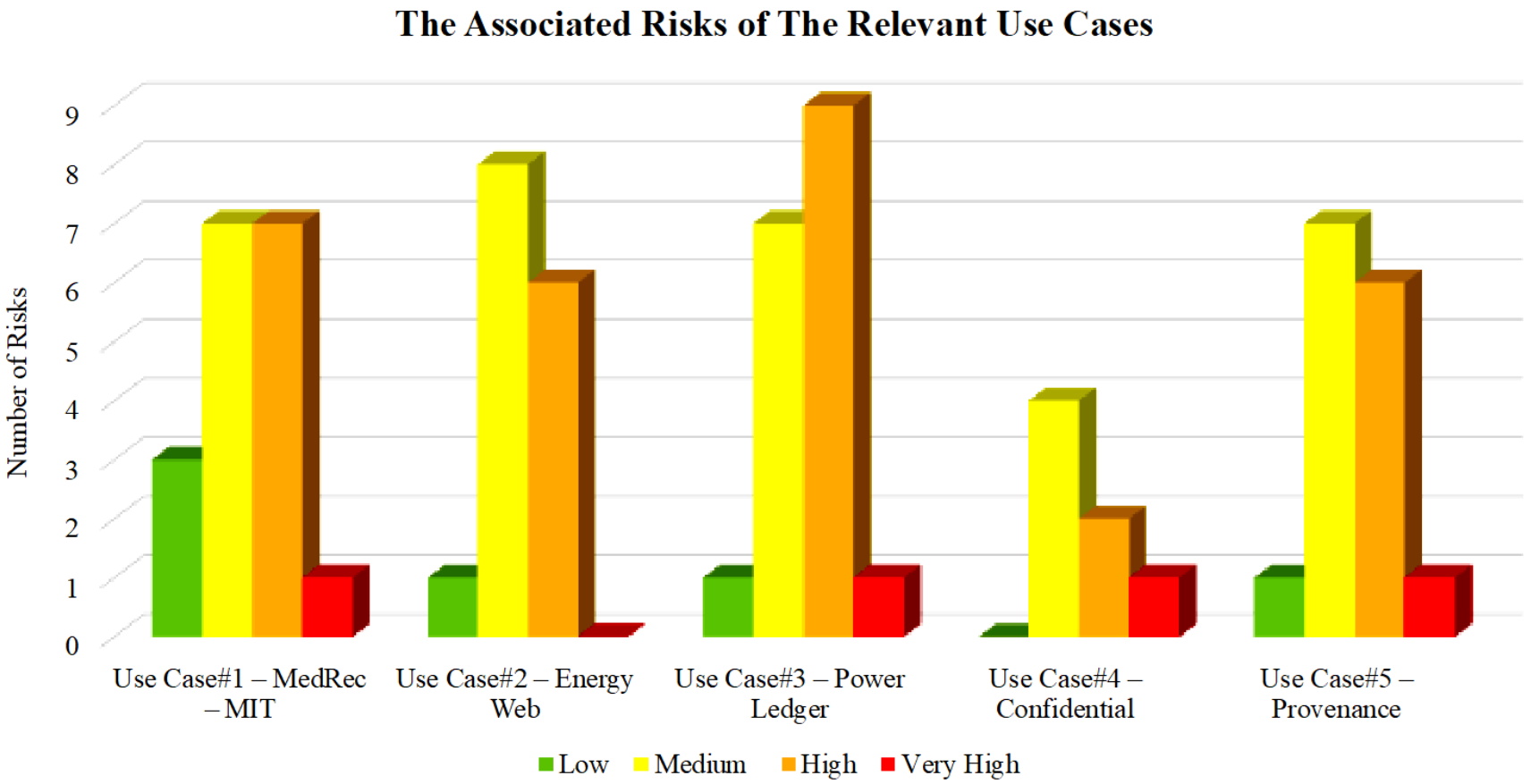


Figure 8: Associated Risks of Blockchain Use Cases (Categorized by Risk Rating)

Since, all relevant use cases are mainly based on blockchain technology, a common risk existed between them is considered as logical. Therefore, there are some risks that are common between them, in other word, the risks that have been mentioned over three use cases or more which are the following. Thus, these risks should be taken into considerations while designing, developing and implementing the blockchain solutions.

- Lack of enforcement for strong security access controls on the patient’s and provider’s nodes to prevent unauthorized access to the respective private key.
- No specified mechanism to protect node's private key from loss.
- No specified mechanism for the node's revocation.
- Lack of the endpoint/node's security along with its relevant applications and software from relevant security threats and vulnerabilities.
- Untested and unaudited smart contracts from the relevant security threats and vulnerabilities prior the deployment.
- Unauthorized access to the smart contract.
- Unspecified requirements for secure communication over the platform and its components.
- Incidents reporting procedure is not specified.
- Unclear vision with respect to data security and confidentiality including but not limited to the block payloads, transmitted data and data at rest.
- Unclear vision on the data type that will be stored on the respective platform.
- Absence of business continuity strategy for the respective platform.
- Lack of the details with the respect to the security of the used cryptographic algorithm against security flaws and vulnerabilities.

- Lack of protection against possible malicious activities of administrators.
- Lack of vision whether the required security assessment against the relevant security threats and vulnerabilities has been performed on the respective platform along with its applications and services before the deployment.
- Unclear vision on the data flow within and between the respective platform and its other linked platforms and applications.

Table 10 show the most security controls (from the ISO27001 security controls, UAE IA security controls and the proposed security controls) that were repeated consistently.

Table 10: Most Repeated Security Controls for Risk Reduction

Most Repeated Security Controls on the Performed Risk Treatment		
ISO27001 Security Controls	**UAE IA Security Controls**	**The proposed security controls**
A.9 Access control	T5 Access Control	UAE-BC-05: Hardware Security Module (HSM)
A.12.6 Technical Vulnerability Management	T7.7 Technical Vulnerability Management	UAE-BC-07: Smart Contract Code Audit
A.18.2 Information security reviews	M5.4.1 Technical Compliance Checking	UAE-BC-03: Data Ownership
A.10 Cryptography	T7.4 Cryptographic Controls	-
-	T5.2.3 User Security Credentials Management	-

Generally, Table 11 shows the consolidated list of the associated risks of the relevant blockchain use cases and their security controls for mitigating them; in order to provide a more generic and summarized approach of the relevant risks related to the blockchain technology and their respective security controls prior implementing any blockchain solution.

Table 11: Consolidated List of the Associated Risks and their Security Controls

Risk ID	Risk Description	Asset Affected	Recommended Security Controls		
			ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-01	Lack of enforcement for strong security access controls on the nodes to prevent unauthorized access to the respective private key.	- User credentials - Respective platform and its components	A.9 Access Control	T5 Access Control	UAE-BC-05: Hardware Security Module (HSM)
R-02	No specified mechanism to protect node's private key from loss.	- User credentials - Respective platform and its components	A9.2.4 Management of Secret Authentication Information of Users	T5.2.3 User Security Credentials Management	UAE-BC-05: Hardware Security Module (HSM)
R-03	No specified mechanism for the node's revocation.	- Abuse the respective platform and its components	A.9.2.1 User Registration and De-Registration A.9.2.2 User Access Provisioning A.9.2.6 Removal or Adjustment of Access Rights	M4.4.3 Removal of Access Rights T5.2.3 User Security Credentials Management	UAE-BC-04: Identity Access Management (IAM)
R-04	Lack of the endpoint/node's security along with its relevant applications and software from relevant security threats and vulnerabilities.	- Node - User credentials - Respective platform and its components	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	UAE-BC-07: Smart Contract Code Audit
R-05	Lack of multi-authentication mechanisms for accessing the relevant databases.	- Database - Data - Respective platform and its components	A9.2 User Access Management	T5.2 User Access Management	-

Table 11: Consolidated List of the Associated Risks and their Security Controls (Continued)

Risk ID	Risk Description	Asset Affected	Recommended Security Controls		
			ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-06	Lack of enforcement for database encryption on the respective nodes in order to prevent data leakage and unauthorized disclosure, modification and/or destruction.	- Database - Data - Respective platform and its components	A.10 Cryptography	T7.4 Cryptographic Controls	UAE-BC-03: Data Ownership
R-07	Lack of database query protection against relevant well known security vulnerabilities.	- Database - Patient Data - Respective platform and its components	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	A.12.6 Technical Vulnerability Management A.18.2 Information security reviews	-
R-08	Absence of the monitoring strategy for the respective platform.	- Respective platform and its components and nodes	T3.6 Monitoring M6 Performance Evaluation and Improvement	A.12.4 Logging and monitoring A.18.2 Information security reviews	UAE-BC-08: Block Publication Rate
R-09	Untested and unaudited smart contracts from the relevant security threats and vulnerabilities prior the deployment.	- Respective smart contract - Respective nodes - Respective platform and its components	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	A.12.6 Technical Vulnerability Management A.18.2 Information security reviews	UAE-BC-07: Smart Contract Code Audit
R-10	Unauthorized access to the smart contract.	- Respective smart contract - Respective nodes - Respective platform and its components	A.9 Access control	T5 Access Control	UAE-BC-06: Smart Contract's Access Control

Table 11: Consolidated List of the Associated Risks and their Security Controls (Continued)

Risk ID	Risk Description	Asset Affected	Recommended Security Controls		
			ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-11	Unclear vision on the used consensus mechanism for signing, verifying and publishing the block on the respective platform.	- Block production - Business processes	-	-	UAE-BC-01: Blockchain Business Processes
R-12	Unspecified requirements for secure communication over the platform and its components.	- Respective platform and its network, applications and nodes components	A.13 Communications Security A.11 Physical and Environmental Security A.9 Access Control	T4 Communications T2 Physical and Environmental Security T5 Access Control	-
R-13	Incidents reporting procedure is not specified.	- Respective platform and its network, applications and nodes components	A.16 Information Security Incident Management	T8 Information Security Incident Management	-
R-14	Unclear vision with respect to data security and confidentiality including but not limited to the block payloads, transmitted data and data at rest.	- Data	A.10 Cryptography	T7.4 Cryptographic Controls	UAE-BC-03: Data Ownership
R-15	Unclear vision on the data type that will be stored on the respective platform.	- Data	-	-	UAE-BC-03: Data Ownership
R-16	Absence of business continuity strategy for the respective platform.	- Respective platform	A.17 Information Security Aspects of Business Continuity Management	T9 Information Systems Continuity Management	-
R-17	Lack of the details with the respect to the security of the used cryptographic algorithm against security flaws and vulnerabilities.	- Data - The chain of the blocks	A.10 Cryptography	T7.4 Cryptographic Controls	-

Table 11: Consolidated List of the Associated Risks and their Security Controls (Continued)

Risk ID	Risk Description	Asset Affected	Recommended Security Controls		
			ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-18	Lack of protection against possible malicious activities of administrators.	- Abuse of privileges - Respective platform and its network, applications and nodes components	A.12.4.3 Administrator and Operator Logs	T3.6.3 Monitoring System Use T3.6.5 Administrator and Operator Logs T5.2.2 Privileges Management	-
R-19	Lack of vision whether the required security assessment against the relevant security threats and vulnerabilities has been performed on the respective platform along with its applications and services before the deployment.	- Respective platform and its components	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-
R-20	Failure to specify and embed the necessary security requirements for the developers to adhere while they are developing and building the relevant solutions, tools and back-end application services on the respective platform.	- Respective platform and its applications, tools and services components	A.14.1 Security Requirements of Information Systems A.12 Operation Security	M5.4 Compliance with Technical Requirements T3 Operations Management	-
R-21	Lack of enforcement for performing the required security assessment (such as threat and vulnerability assessment) of the developed solutions, tools and back-end application services before deploying them on the respective platform.	- Respective platform and its applications, tools and services components	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-

Table 11: Consolidated List of the Associated Risks and their Security Controls (Continued)

Risk ID	Risk Description	Asset Affected	Recommended Security Controls		
			ISO 27001 Controls	UAE IA Standard Controls	The Proposed Controls
R-22	Lack of security vision on the specified APIs and whether it has been tested against the relevant security threats, vulnerabilities, bugs and holes, and data breaches and DoS attack as well.	- Data - Respective platform and its components	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-
R-23	Unclear vision on the data flow within and between the respective platform and its other linked platforms and applications.	- Data	A.13 Communications Security	T4 Communications	-
R-24	Unclear vision with the respect of the security level of the relevant servers including but not limited to physical security, patching and server maintenance, event logs, system integrity control, anti-virus and anti-malware, authentication and access controls, and backups and restore.	- Respective server	A.11 Physical and Environmental Security A.12 Operation Security A.14 System Acquisition, Development and Maintenance A.9 Access Control	T2 Physical and Environmental Security T3 Operations Management T7 Information Systems Acquisition, Development and Maintenance T5 Access Control	-
R-25	Unclear vision on how the key pair that reside on the respective network are protected against hacking, theft, malicious activities and unauthorized access.	- User credentials - Respective platform and its components	A.9 Access Control A.10 Cryptography	T5 Access Control T7.4 Cryptographic Controls	UAE-BC-05: Hardware Security Module (HSM)
R-26	Lack of the security requirements enforcement while the developers are configuring the respective Docker images such as but not limited to threat and vulnerability management, patch management and etc.	- Respective Docker images - Respective platform and its components	A.12.6 Technical Vulnerability Management A.18.2 Information Security Reviews A.12 Operation Security	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking T3 Operations Management	-

As per the performed risk assessment and treatment on the relevant blockchain use cases, it shown that there are some risks that can be mitigated and reduced through the proposed security controls that are mainly focuses on the blockchain technology due to the lack of blockchain security controls in International and National Information Security Standards such as the ISO 27001 Standard's controls and UAE IA Standard's controls. In addition, some of the proposed security controls are considered as complementary along with the existed security controls from the relevant information security standards to achieve the expected risk reduction successfully.

5.1 Proposed Evaluation Process

With the respect to evaluating the effectiveness of the proposed security controls, it requires real implementation of these controls by an organization through establishing and implementing relevant procedure. Therefore, this section provides briefly further information with regard to this aspect along with a high-level relevant process; as a guideline for organizations.

The effectiveness of the implemented Information Security controls (as part of the Information Security Management System (ISMS)) must be assessed in a consistent and repeatable manner, in line with International Standards such as ISO/IEC 27004:2016, in order to obtain assurance that the implemented controls continue to operate as intended in protecting the organization's information assets. The organization should ensure that cost-effective, comparable, and repeatable measurements are used for assessing the security controls, in order to provide the management with the assurance that people, process, and technology that contribute towards Information Security are effective. The relevant measurements also provide

the management with a clear understanding of the existing Information Security risks and the recommendations to manage those risks. Measurement of effectiveness of Information Security controls will hence ensure that the Information Security Management System (ISMS) is measured, analyzed, evaluated, and improved on a continuous basis.

Moreover, the following is a high-level evaluation process for measuring the effectiveness of the security controls implementation in line with International Standards such as ISO/IEC 27004:2016.

1) As part of the annual risk assessment carried out by the organization, all risks should be mapped to their corresponding ISO 27001 and UAE IA controls.
2) Based on the severity of the risk levels, the effectiveness of the controls should be assessed based on a predefined evaluation criteria. For example, as shown in Table 12.

Table 12: Control Effectiveness Matrix

Risk Level	**Control Effectiveness Score**
Very Low	Fully Effective
Low, Medium	Partially Effective
Very High, High	Not Effective

3) Based on the control effectiveness score assigned to each control, the corrective action plans should be prioritized for implementation. For example, as shown in Table 13.

Table 13: Corrective Action Prioritization

Control Effectiveness Score	**Corrective Action Implementation Timeline**
Fully Effective	N/A
Partially Effective	Within 3 months
Not Effective	Within 1 month

4) The control effectiveness scores along with the corrective action plans should be presented to and agreed upon with the information security committee.
5) The corrective action plans should be implemented by all stakeholders “for example, the respective departments” within the agreed timelines.
6) The stakeholders should keep the information security committee informed about the progress of any corrective action plans and any potential delays and/or issues.
7) The progress on the corrective actions should be reviewed during the information security committee meetings. In addition, the enhancements/adjustments to the plan may be made, as applicable.

Chapter 6: Conclusions and Future Work

In summary, this thesis aims to establish new information security controls specifically related to the blockchain technology in order to mitigate the relevant information security risks and consequently protecting the information and information assets against unauthorized disclosure, modification, and destruction that could have negatively impact at individuals, entities and/or national levels.

The proposed security controls are not covered by International and National Information Security Standards i.e., the ISO 27001:2013 Standard and the UAE Information Assurance Standards developed by the Signals Intelligence Agency (formerly known as the National Electronic Security Authority). The risk assessment and treatment have been performed on five blockchain use cases (following ISO 31000:2018 – Risk Management Standard Guidance) to determine their involved risks along with their respective security controls from the UAE IA Standard's controls, ISO 27001 Standard's controls and the proposed security controls. The results showed that there are some risks that can be mitigated and reduced through the proposed security controls and the lack of the relevant security controls in the relevant International and National Information Security Standards. In addition, some of the proposed security controls are considered as complementary along with the existed security controls from the relevant information security standards.

The research limitations were failure to receive the required documentation regarding the blockchain use cases that are implemented in UAE from the respective providers (except for one of the relevant cases). Therefore, the majority of the used blockchain use cases on this thesis are publicly published papers that have lacking on the technical details about the respective solutions; which could have an effect on the

risk assessment results on the relevant use cases due to the inability to perform a comprehensive Risk Identification properly.

Finally, in order to evaluate the effectiveness of the proposed security controls on the blockchain solution into reducing the associated risks level to the lowest rate and ensuring that they will not introduce new risks that may negatively impact on the overall security of the blockchain solution. Therefore, the next step firstly will be performing the risk assessment and treatment (through selecting the appropriate proposed security controls) on a number of blockchain solutions in order to ensure that the proposed security controls are applicable for any blockchain solution regardless size, nature, complexity, architecture and etc. Then the selected proposed security controls require real implementation on the relevant blockchain solutions. Lastly, the relevant evaluation procedure/process will be established and implemented to determine the effectiveness and success of the proposed security controls that are in place. In addition, the future work will focus on generally establishing the security controls according to the associated risks of a specific blockchain use cases such as but not limited to finance, supply chain, digital identity, energy, healthcare, and government; in order to ensure the comprehensive coverage of the blockchain risks.

References

[1] R. M. Linda and J. Pawczuk, "Deloitte's 2019 Global Blockchain Survey," 2019. [Online]. Accessed on: February 25, 2020. Available: https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf

[2] Z. Liu and Z. Li, "A blockchain-based framework of cross-border e-commerce supply chain," International Journal of Information Management, vol. 52, pp. 59-71, 2020.

[3] Z. Wang, T. Wang, H. Hu, J. Gong, X. Ren, and Q. Xiao, "Blockchain-based framework for improving supply chain traceability and information sharing in precast construction," Automation in Construction, vol. 111, pp. 63-75, 2020.

[4] V. K. Manupati, T. Schoenherr, M. Ramkumar, S. M. Wagner, S. K. Pabba, and R. Inder Raj Singh, "A blockchain-based approach for a multi-echelon sustainable supply chain," International Journal of Production Research, vol. 58, no. 7, pp. 2222-2241, 2020.

[5] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized Authentication of Distributed Patients in Hospital Networks using Blockchain," IEEE Journal of Biomedical and Health Informatics, vol. 122, no. 14, pp. 26-37, 2020.

[6] J. Fu, N. Wang, and Y. Cai, "Privacy-Preserving in Healthcare Blockchain Systems Based on Lightweight Message Sharing," Sensors, vol. 20, no. 7, pp. 1898-1908, 2020.

[7] Z. Wang, N. Luo, and P. Zhou, "GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare," Journal of Parallel and Distributed Computing, vol. 23, pp. 58-67, 2020.

[8] G. van Leeuwen, T. AlSkaif, M. Gibescu, and W. van Sark, "An integrated blockchain-based energy management platform with bilateral trading for microgrid communities," Applied Energy, vol. 263, pp. 114-128, 2020.

[9] O. Van Cutsem, D. H. Dac, P. Boudou, and M. Kayal, "Cooperative energy management of a community of smart-buildings: A Blockchain approach," International Journal of Electrical Power & Energy Systems, vol. 117, pp. 105-119, 2020.

[10] O. Samuel, A. Almogren, A. Javaid, M. Zuair, I. Ullah, and N. Javaid, "Leveraging Blockchain Technology for Secure Energy Trading and Least-Cost Evaluation of Decentralized Contributions to Electrification in Sub-Saharan Africa," Entropy, vol. 22, no. 2, pp. 226-238, 2020.

[11] K. Otto, "Data standards are fundamental for blockchain implementation," National Provisioner, vol. 233, no. 10, pp. 80-89, 2019.

[12] D. Nusi, D. A. Aranda, and V. Stantchev, “Perspectives on risks and standards that affect the requirements engineering of blockchain technology,” Computer Standards & Interfaces, vol. 69, pp. 103-119, 2020.

[13] A. L. Avivah, "Hype Cycle for Blockchain Technologies," 2020. [Online]. Accessed on: July 13, 2020. Available: https://www.gartner.com/en/documents/3987450/hype-cycle-for-blockchain-technologies-2020.

[14] Chainstack, "Hype Cycle for Blockchain Technologies," 2020. [Online]. Accessed on: June 2, 2020. Available: https://pages.chainstack.com/hype-cycle-for-blockchain-technologies-2020.

[15] Smartdubai, "Blockchain," [Online]. Accessed on: April 19, 2020. Available: https://www.smartdubai.ae/initiatives/blockchain.

[16] UAE Government, "Emirates Blockchain Strategy 2021," 2020. [Online]. Accessed on: April 27, 2020. Available: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/emirates-blockchain-strategy-2021.

[17] M. E. Cornelius and C. Agbo, "Blockchain Technology in Healthcare: A Systematic Review," Healthcare, vol. 7, no. 2, pp. 102-115, 2019.

[18] M. T. Xiaolin, "Electronics Supply Chain Integrity Enabled by Blockchain," ACM Transactions on Design Automation of Electronic Systems (TODAES), vol. 27, no. 3, pp. 1-25, 2019.

[19] A. Ihab, "Cybersecurity Risks of Blockchain Technology," International Journal of Computer Applications, vol. 177, no. 42, pp. 8-14, 2020.

[20] V. Chang, "McAfee Highlights Blockchain Cybersecurity Risks," Computer Security Update, vol. 19, no. 7, pp. 28-37, 2018.

[21] G. Gaby, J. Mohler, M. Milojkovic, and P. B. Marella, “Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology,” Sustainable Cities and Society, vol. 39, pp. 283-297, 2018.

[22] C. Lima, “Developing Open and Interoperable DLT$\backslash$/Blockchain Standards,” Computer, vol. 51, no. 11, pp. 106-111, 2018.

[23] F. John and M. Adrian, “Blockchain’s future: can the decentralized blockchain community succeed in creating standards?,” The Knowledge Engineering Review, vol. 35, pp. 25-37, 2020.

[24] T. M. Kiran, Risk and Control Considerations for Blockchain Technology, 2nd edition. UK, CohnReznick Publisher, 2018.

[25] G. Vincent and S. Mark, “Blockchain Standard: Can We Reach Consensus?,” IEEE Communications Standards Magazine, vol. 2, no. 3, pp. 16-21, 2018.

[26] B. Rafael and N. Rocco, “Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards,” IEEE Communications Standards Magazine, vol. 2, no. 3, pp. 22-28, 2018.

[27] P. James and V. Maria, “Blockchain Compliance with Federal Cryptographic Information-Processing Standards,” IEEE Security & Privacy, vol. 18, no. 1, pp. 65-70, 2020.

[28] ISO, "ISO 31000:2018(en) Risk Management-Guidelines,". [Online]. Accessed on: May 19, 2020. Available: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

[29] MedRec, "Architecture of MedRec 2.0" [Online]. Accessed on: March 20, 2019. Available: https://medrec.media.mit.edu/technical/.

[30] N. Gavhane, "EW-DOS: Technology Detail," 2020. [Online]. Accessed on: June 7, 2020. Available: https://www.energyweb.org/reports/ewdos-technology-detail/.

[31] Powerledger, "Pwer Ledger Whitepaper," 2019. [Online]. Accessed on: Nov. 14, 2019. Available: https://www.powerledger.io/wp-content/uploads/2019/11/power-ledger-whitepaper.pdf

[32] Provenance, "Provenance white paper," 2020. [Online]. Accessed on: April 2, 2020. Available: https://www.provenance.io/documents/Provenance%20Whitepaper%20-%202020.pdf.

Appendix

Standards Developing Organizations	DLT/Blockchain Standards	Status	Source
International Organization for Standardization (ISO)	1) ISO/CD TR 3242: *Use cases*	Under development	https://www.iso.org/committee/6266604.html
	2) ISO/FDIS 22739: *Vocabulary*	Published on July 2020	
	3) ISO/PRF TR 23244: *Privacy and personally identifiable information protection considerations*	Published on May 2020	
	4) ISO/CD TR 23245.2: *Security risks, threats and vulnerabilities*	Under development	
	5) ISO/CD 23257.3: *Reference architecture*	Under development	
	6) ISO/WD TS 23258: *Taxonomy and Ontology*	Under development	
	7) ISO/AWI TS 23259: *Legally binding smart contracts*	Under development	
	8) ISO/TR 23455:2019: *Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems*	Published on September 2019	
	9) ISO/CD TR 23576: *Security management of digital asset custodians*	Under development	
	10) ISO/AWI TS 23635: *Guidelines for governance*	Under development	
IEEE Standards Association	1) 2418.2-2020: *IEEE Approved Draft Standard Data Format for Blockchain Systems*	Published	https://standards.ieee.org/search-results.html?facetValue=4294967245,4294967230,4294967250&q=Standard
	2) P2140.1: *Standard for General Requirements for Cryptocurrency Exchanges*	Under development	
	3) P2140.3: *Standard for User Identification and Anti-Money Laundering on Cryptocurrency Exchanges*	Under development	

Standards Developing Organizations	DLT/Blockchain Standards	Status	Source
	4) P2140.4: *Standard for Distributed/Decentralized Exchange Framework using DLT (Distributed Ledger Technology)*	Under development	
	5) P2140.5: *IEEE Draft Standard for Custodian Framework of Cryptocurrency*	Published	
	6) P2140.2: *Standard for Security Management for Customer Cryptographic Assets on Cryptocurrency Exchanges*	Under development	
	7) P2141.1: *Standard for the Use of Blockchain in Anti-Corruption Applications for Centralized Organizations*	Under development	
	8) P2141.2: *Standard for Transforming Enterprise Information Systems from Centralized Architecture into Blockchain-based Decentralized Architecture*	Under development	
	9) P2141.3: *Standard for Transforming Enterprise Information Systems from Distributed Architecture into Blockchain-based Decentralized Architecture*	Under development	
	10) P2143.1: *IEEE Draft Standard for General Process of Cryptocurrency Payment*	Published	
	11) P2143.2: *Standard for Cryptocurrency Payment Performance Metrics*	Under development	
	12) P2143.3: *Standard for Risk Control Requirements for Cryptocurrency Payment*	Under development	
	13) P2144.1: *Standard for Framework of Blockchain-*	Under development	

Standards Developing Organizations	DLT/Blockchain Standards	Status	Source
	based Internet of Things (IoT) Data Management		
	14) P2144.2: *Standard for Functional Requirements in Blockchain-based Internet of Things (IoT) Data Management*	Under development	
	15) P2144.3: *Standard for Assessment of Blockchain-based Internet of Things (IoT) Data Management*	Under development	
	16) P2418.10: *Standard for Blockchain-based Digital Asset Management*	Under development	
	17) P2418.7: *Standard for the Use of Blockchain in Supply Chain Finance*	Under development	
	18) P2418.9: *Standard for Cryptocurrency Based Security Tokens*	Under development	
	19) P2418.1: *Standard for the Framework of Blockchain Use in Internet of Things (IoT)*	Under development	
	20) P2418.5: *Standard for Blockchain in Energy*	Under development	
	21) P2418.8: *Standard for Blockchain Applications in Governments*	Under development	
	22) P2142.1: *Recommended Practice for E-Invoice Business Using Blockchain Technology*	Under development	

جامعة الإمارات العربية المتحدة
United Arab Emirates University
UAEU Libraries
DigitizationDepatment
United Arab Emirates
Digitally signed by Shrieen
DN: cn=Shrieen, o=United Arab Emirates University, ou=UAEU Library Digitizatio, email=shrieen@uaeu.ac.ae, c=AE
Date: 2021.08.23 11:18:16 +04'00'